Prof. Dr. Friedrich Kasch
Prof. Dr. Bodo Pareigis

Grundbegriffe der Mathematik

Ein Begleittext für das Studium der Mathematik

4. Auflage

Verlag Reinhard Fischer München

CIP-Kurztitelaufnahme der Deutschen Bibliothek

Kasch, Friedrich
Grundbegriffe der Mathematik: e. Begleittext für das Studium d. Mathematik/Friedrich Kasch; Bodo Pareigis.
– 3. überarb. Auflage – München: R. Fischer 1986
ISBN 3-88927-030-1
NE: Pareigis, Bodo:
27

Anschrift der Autoren:
Prof. Dr. Friedrich Kasch,
Prof. Dr. Bodo Pareigis
Mathematisches Institut der
Ludwig-Maximilians-Universität München
Theresienstr. 39
8000 München 2

4. Auflage 1991

ISBN 3-88927-030-1

Druck und Bindung: Novotny, Söcking

Vorwort

Als Leser dieses Buches stellen wir uns Studenten der Mathematik, Mathematiklehrer und mathematisch interessierte Schüler vor.

In erster Linie wendet es sich an Studienanfänger der Mathematik. In den Anfängervorlesungen müssen eine Reihe von Begriffen benutzt werden, für deren ausführliche Behandlung in den Vorlesungen selbst kaum Zeit zur Verfügung steht. Daher werden hier vor allem solche Grundbegriffe dargestellt, die nicht zu den Hauptinhalten dieser Vorlesungen gehören. Wir stellen uns daher auch nicht vor, daß ein Studienanfänger dieses Buch sogleich im Zusammenhang von vorn bis hinten durchlesen muß. Er kann vielmehr diejenigen Abschnitte lesen, die in der Vorlesung angesprochen werden. Auf diese Weise soll das Buch als Begleittext neben der Vorlesung Verwendung finden und außerdem die zahlreichen Querverbindungen zwischen den verschiedenen mathematischen Vorlesungen deutlicher werden lassen. Wir hoffen, daß dieses Buch dem Leser schließlich insgesamt einen guten Eindruck von den Prinzipien des Aufbaus der Mathematik vermitteln wird.

Im ersten Kapitel werden Grundbegriffe der Logik dargestellt, wobei es uns nicht nur darauf ankommt, den Gebrauch der logischen Symbole einzuführen, sondern auch einen ersten Eindruck von der Möglichkeit der Mathematisierung und Formalisierung des logischen Schließens zu geben. Erfahrungsgemäß macht es gerade dem Anfänger große Schwierigkeiten, mathematisch-logische Aussagen nur mit den Hilfsmitteln der naiven Logik zu verknüpfen oder zu negieren. Hier kann häufig nur die Formalisierung der Aussagen helfen. Der daran interessierte Leser kann dadurch angeregt werden, an Hand von Spezialdarstellungen tiefer in die mathematische Logik einzudringen.

Das zweite Kapitel behandelt die Grundbegriffe der Mengenlehre. Es verfolgt wie das erste Kapitel zwei Ziele. Zunächst soll die Sprache der Mengenlehre, die heute „Umgangssprache" der Mathematik ist, eingeführt werden. Gleichzeitig aber soll ein Eindruck von der Mengenlehre als einer eigenständigen, interessanten und wichtigen mathematischen Theorie gegeben werden. In einem weiteren Abschnitt haben wir eine Einführung in die Kardinal- und Ordinalzahlen aufgenommen.

In den nächsten drei Kapiteln behandeln wir dann mathematische Grundstrukturen (im Sinne von Bourbaki) und zwar Relationen

(insbesondere Abbildungen, Äquivalenzrelationen und Ordnungen), algebraische Strukturen und topologische Räume.

Das folgende Kapitel über Kategorien zeigt, daß die Einteilung in Grundstrukturen nicht als ein starres Schema zu betrachten ist, sondern daß es hier Übergänge und Gemeinsamkeiten gibt, die dieses Einteilungsschema in gewissem Sinne wieder aufheben. Eines der Hauptanliegen der Theorie der Kategorien ist es gerade, das Gemeinsame verschiedener Strukturen herauszustellen.

Schließlich geben wir im letzten Kapitel eine detaillierte Darstellung des Aufbaus des Zahlensystems, wobei von den Peanoschen Axiomen ausgegangen wird. Unter Verwendung von Eigenschaften der rekursiven Funktionen führen wir die Rechengesetze der natürlichen Zahlen ein. Die reellen Zahlen werden sowohl mit Cauchy-Folgen als auch mit Dedekindschen Schnitten konstruiert. Es wird die Äquivalenz dieser beiden Konstruktionsmöglichkeiten nachgewiesen. Im Anschluß daran stellen wir einen weiteren üblicherweise nicht erwähnten Zahlenbereich, den der Quaternionen, vor.

Wenn wir bisher vor allem Mathematikstudenten angesprochen haben, so entspricht dies der Entstehung des Buches. Es ist aus einer Vorlesungsausarbeitung zu den Anfängervorlesungen hervorgegangen.

Wir hoffen jedoch, daß es auch für Mathematiklehrer geeignet sein kann, die sich über den neuesten Stand der Auffassung und Formulierung der Grundbegriffe informieren wollen.

Für mathematisch interessierte Schüler mag es einen Eindruck von dem geben, was Mathematik als eine in rascher Entwicklung befindliche Wissenschaft ist. Wir haben dabei Wert darauf gelegt, daß die verschiedenen Kapitel im wesentlichen unabhängig voneinander gelesen werden können. Als eine Grundvoraussetzung muß allerdings eine gewisse Vertrautheit mit den Begriffen „Menge" und „Abbildung" vorhanden sein, etwa auf dem Niveau wie diese Begriffe in den Kollegstufen der Gymnasien heute verwendet werden.

Wir freuen uns, daß wir hiermit der Öffentlichkeit die dritte Auflage dieses Begleittextes vorlegen können und danken dem Verlag Reinhard Fischer für seine aktive Unterstützung.

München im Juli 1986

Die Verfasser

Inhalt

I. Kapitel: Logische Grundbegriffe

II. Kapitel: Grundbegriffe der Mengenlehre

III. Kapitel: Relationen

IV. Kapitel: Algebraische Strukturen

V. Kapitel: Metrische und topologische Räume

VI. Kapitel: Kategorien und Funktoren

VII. Kapitel: Aufbau des Zahlensystems

I. Kapitel: Logische Grundbegriffe

§ 1 Aussagenlogik

1.1 Aussagen und ihre Verknüpfungen

In der Mathematik und in anderen Bereichen, in denen logisch argumentiert wird, interessiert der Wahrheitsgehalt der verwendeten Sätze. Was das bedeutet, soll im folgenden präzisiert werden.

Ist es sinnvoll, bei einem Satz danach zu fragen, ob er w a h r (w) oder f a l s c h (f) ist, so wollen wir ihn eine A u s s a g e nennen. Zum Beispiel sind " 5 ist eine Primzahl " und " New York ist die Hauptstadt von England " Aussagen, während " Wann kommst Du ? " und " Sei x eine Primzahl " keine Aussagen sind.

Aus vorgegebenen Aussagen kann man weitere Aussagen durch logische Verknüpfungen, auch J u n k t o r e n genannt, erhalten. Wir besprechen im folgenden eine einstellige Verknüpfung, die N e g a t i o n , und mehrere zweistellige Verknüpfungen, die K o n j u k t i o n , die D i s j u n k t i o n , die S u b j u n k t i o n und die B i j u n k t i o n . Es gibt noch weitere ein- und zweistellige Verknüpfungen, die uns hier jedoch nicht interessieren. Alle diese Verknüpfungen sind in der Umgangssprache mehr oder weniger bekannt und erscheinen dort in vielfältiger Form. Wir werden zur Präzisierung für die Verknüpfungen Abkürzungen, sogenannte logische Zeichen, einführen. Ein weiterer Vorteil der Verwendung der Abkürzungen besteht darin, daß logische Prozesse, wie zum Beispiel Beweise, formal mit den einzuführenden logischen Zeichen angegeben werden können, ohne auf den Inhalt einzugehen.

Die N e g a t i o n wird umgangssprachlich durch die Verneinung einer Aussage ausgedrückt, etwa durch " Es ist nicht der Fall, daß ... ". Die Negation von " 5 ist eine Primzahl " ist " Es ist nicht der Fall, daß 5 eine Prim-

zahl ist ". Häufig sagt man dann einfach " 5 ist keine Primzahl ". Das logische Zeichen für die Negation ist " ¬ " , genannt " non ". Ist also A eine Aussage, so ist ¬ A ihre Negation. Die Negation ist somit eine Verknüpfung, die aus einer Aussage eine neue Aussage macht. Im Gegensatz zu den später zu besprechenden Verknüpfungen, die aus zwei Aussagen eine neue Aussage machen und die daher zweistellige Verknüpfungen heißen, nennt man die Negation eine einstellige Verknüpfung. Die anfangs aufgeworfene Frage nach dem Wahrheitsgehalt einer Aussage wird für die Negation und die weiteren Verknüpfungen im folgenden Abschnitt besprochen.

Die K o n j u k t i o n , eine zweistellige Verknüpfung, wird umgangssprachlich durch "... und ..." oder " Sowohl ... als auch ..." ausgedrückt. Dabei ist es für die Zulässigkeit dieser Verknüpfung gleichgültig, ob die zu verknüpfenden Aussagen wahr oder falsch sind und ob ihre Inhalte miteinander in Beziehung stehen. Beliebige Aussagen dürfen durch die Konjuktion verknüpft werden. So wird aus der Aussage " 5 ist eine Primzahl " und der weiteren Aussage " New York ist die Hauptstadt von England " durch Anwendung der Konjunktion die Aussage " 5 ist eine Primzahl und New York ist die Hauptstadt von England ". Das logische Zeichen für die Konjunktion ist " ∧ ", bezeichnet mit " und ". Sind A und B Aussagen, so ist ihre Konjunktion A ∧ B eine neue Aussage, das heißt, es ist wieder sinnvoll zu fragen, ob A ∧ B wahr oder falsch ist.

Die D i s j u n k t i o n wird umgangssprachlich durch " ... oder ... " ausgedrückt. Sie ist wie die Konjunktion eine zweistellige Verknüpfung. Zu betonen ist, daß die Disjunktion " ... oder ... " nicht im Sinne des ausschließenden " entweder ... oder ... " verwendet wird. Die durch die Verknüpfung mit " oder " entstehende neue Aussage ist also auch dann wahr, wenn beide durch " oder " verbundenen Aussagen wahr sind. In diesem Sinne ist zum Beispiel die Disjunktion von " Max hat blaue Augen " und " Moritz hat blonde Haare ", also " Max hat blaue Augen oder Moritz hat blonde Haare ", auch dann wahr, wenn sowohl

Max blaue Augen hat, als auch Moritz blonde Haare hat. Das logische Zeichen für die Disjunktion ist " $\vee$ ", bezeichnet mit " oder ". Sind A und B Aussagen, so ist ihre Disjunktion $A \vee B$ eine neue Aussage.

Die S u b j u n k t i o n wird umgangssprachlich auf sehr vielfältige Weise ausgedrückt. Sind A und B Aussagen, so wird die Subjunktion zwischen A und B ausgedrückt durch

" Aus A folgt B "
" A impliziert B "
" Wenn A, dann B "
" A nur dann, wenn B "
" B dann, wenn A "
" B, falls A "
" A ist eine hinreichende Bedingung für B "
" A hinreichend für B "
" B ist eine notwendige Bedingung für A "
" B ist notwendig für A " .

Alle diese Formulierungen werden wir als gleichbedeutend verwenden. Der Leser mache sich die jeweilige umgangsspraliche Bedeutung für den Fall klar, daß A die Aussage " John ist ein Engländer " und B die Aussage " John ist ein Mensch " sind. Als logisches Zeichen für die Subjunktion verwenden wir " $\Longrightarrow$ ", genannt " wenn ..., so ... ". Sind A und B Aussagen, so ist also ihre Subjunktion $A \Rightarrow B$ wieder eine Aussage.

Einige Autoren bezeichnen die Subjunktion auch als Implikation. Andere reservieren die Bezeichnung Implikation für die Subjunktion, sofern diese eine Tautologie (siehe 1.4) ist. Also Vorsicht ! Beim Lesen von Literatur die jeweilige Notation beachten.

Die B i j u n k t i o n erscheint in der Umgangssprache - ebenso wie die Subjunktion - in vielfältiger Weise. Aus den Aussagen A und B wird durch Bijunktion eine der folgenden Aussagen, die alle die gleiche Bedeutung haben:

" A ist gleichbedeutend mit B "
" A ist äquivalent zu B "

" A dann und nur dann, wenn B "

" A impliziert B und B impliziert A "

" A ist notwendig und hinreichend für B ".

Im täglichen Leben treten Bijunktionen nur selten und in mehr oder weniger trivialem Zusammenhang auf. In der Mathematik ist es jedoch häufig das Hauptziel eines Beweises zu zeigen, daß zwei Aussagen äquivalent sind. Der Leser mache sich die Bedeutung der Bijunktion an den Aussagen " John lebt " und " John wurde geboren, ist aber noch nicht gestorben " klar. Als logisches Zeichen für die Bijunktion verwenden wir " $\Leftrightarrow$ "; also wird aus den Aussagen A und B durch Bijunktion die Aussage $A \Leftrightarrow B$.

Wir beenden diesen Abschnitt mit einem etwas komplizierteren Beispiel. Die Aussage " Wenn Bayern München oder Werder Bremen verlieren, und wenn Schalke 04 gewinnt, dann wird Eintracht Frankfurt deutscher Meister und ich werde außerdem eine Wette verlieren " läßt sich in unserem Formalismus durch

$$((B \vee W) \wedge S) \Rightarrow (F \wedge I) \ .$$

Häufig können bei solchenAusdrücken umfangreiche Klammerungen auftreten. Wie bei den algebraischen Rechenoperetionen, zum Beispiel $a \cdot b + c = (a \cdot b) + c$, einigt man sich auch hier auf eine gewisse Reihenfolge der Durchführung der Verknüpfungen, wenn diese nicht durch Klammern eindeutig festgelegt ist. Die Negation " $\neg$ " ist zuerst auszuführen. Dann folgen Konjunktion " $\wedge$ " und Disjunktion " $\vee$ ", wobei keine vor der anderen Vorrang hat. Danach erst ist die Subjunktion " $\Rightarrow$ " durchzuführen. Am schwächsten bindet schließlich die Bijunktion " $\Leftrightarrow$ ". Die obige Formel kann unter Beachtung dieser Regeln auch geschrieben werden als

$$(B \vee W) \wedge S \Rightarrow F \wedge I \ .$$

Ein weiteres Beispiel ist

$$A \wedge \neg B \Rightarrow C \Leftrightarrow \neg A \vee B \vee C \ ,$$

was ausführlich

$$((A \wedge (\neg B)) \Rightarrow C) \Leftrightarrow (((\neg A) \vee B) \vee C)$$

bedeutet. Wegen einer späteren Regel ist $(A \vee B) \vee C$ dasselbe wie $A \vee (B \vee C)$, so daß man auch diese Klammern weglassen kann. Beispielsweise haben jedoch $(A \wedge B) \vee C$ und $A \wedge (B \vee C)$ verschiedene Bedeutung.

1.2 Aussageformen, Wahrheitstafeln der Junktoren

Aus der Definition der Verknüpfungen ebenso wie aus einigen Beispielen sieht man, daß die Verknüpfungen auch auf Aussagenpaare angewendet werden können, die keinen ersichtlichen inhaltlichen Zusammenhang haben. So können wir zum Beispiel die Aussage bilden:"Wenn der Mond rund ist, hat Moritz blonde Haare". In der Umgangssprache wird es bei dieser Aussage zweifelhaft sein, ob man sie als wahr oder falsch betrachten soll, selbst wenn man sich von der Wahrheit der Aussagen "Der Mond ist rund" und "Moritz hat blonde Haare" überzeugt hat. Um aber den Wahrheitswert der Verknüpfung von ein oder zwei Aussagen in jedem Falle genau zu kennen, muß man sich von der inhaltlichen Bedeutung der Aussagen lösen und nur ihren Wahrheitswert betrachten. Nach sogenannten W a h r h e i t s t a f e l n kann man dann in jedem Falle den Wahrheitswert der verknüpften Aussage bestimmen. Somit lösen wir uns hier auch von der ursprünglichen inhaltlichen Bedeutung der Verknüpfung und sehen im folgenden die Bestimmung der Wahrheitswerte als Hauptaufgabe an. Die folgenden Wahrheitstafeln können daher als Definition der Verknüpfungen angesehen werden, auch wenn wir sie mit inhaltlichen Argumenten und Beispielen motiviert haben.

Zur Aufstellung der Wahrheitstafeln führen wir A u s s a g e v a r i a b l e n P, Q, R,... ein. Nach Bedarf können für diese Variablen sowohl wahre als auch falsche Aussagen eingesetzt werden. Aussagevariablen können ebenso wie die Aussagen durch die logischen Zeichen verknüpft werden, wie zum Beispiel $\neg P$, $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$, $P \Leftrightarrow Q$. Aussagevariablen und alle damit durch Anwendung der Junktoren gebildeten Ausdrücke sollen A u s s a g e f o r m e n genannt werden. Ersetzt man in einer Aussageform alle Aussagevariablen durch Aussagen, dann erhält man offenbar

wieder eine Aussage. Umgekehrt erhält man aus einer Aussage eine Aussageform, indem man in der Aussage jede Teilaussage durch eine Aussagevariable ersetzt.

Es sollen nun die W a h r h e i t s t a f e l n angegeben werden.
Wahrheitstafel der Negation:

P	$\neg$ P
w	f
f	w

Das bedeutet: Wird für P eine wahre Aussage A eingesetzt, so ist $\neg$ A falsch; wird für P eine falsche Aussage A eingesetzt, so ist $\neg$ A wahr.

Wahrheitstafel der Konjunktion:

P	Q	P $\wedge$ Q
w	w	w
w	f	f
f	w	f
f	f	f

Wahrheitstafel der Disjunktion:

P	Q	P $\vee$ Q
w	w	w
w	f	w
f	w	w
f	f	f

Hier sehen wir, daß nicht nur für ein wahres A und falsches B bzw. ein falsches A und wahres B die Disjunktion A $\vee$ B wahr ist (2. und 3. Zeile); wie schon erwähnt, ist auch im Falle, daß A und B beide wahre Aussagen sind, A $\vee$ B eine wahre Aussage. Hierin äußert sich die Definition von $\vee$ (oder) im nicht-ausschließenden Sinne. (Für " oder " im ausschließenden Sinne wäre für wahre A und B " A oder B " falsch !)

Wahrheitstafel der Subjunktion:

P	Q	$P \Rightarrow Q$
w	w	w
w	f	f
f	w	w
f	f	w

Bei der Subjunktion wird zum Ausdruck gebracht, daß Q auf irgendeine Weise aus P hervorgeht. Sicher ist das nicht der Fall, wenn für P eine wahre und für Q eine falsche Aussage stehen. Daher der Wahrheitswert f in diesem Falle (2. Zeile). Steht für Q eine wahre Aussage, so ist es gewissermaßen gleichgültig, wie sie erhalten worden ist, insbesondere ob für P eine wahre oder falsche Aussage eingesetzt worden ist. Damit erklärt sich die erste und dritte Zeile der Wahrheitstafel. Um die letzte Zeile zu rechtfertigen, betrachte man die Aussage $A \Rightarrow A$. Diese Aussage sollte unabhängig davon wahr sein, welchen Wahrheitswert A hat. Ist A falsch, so folgt aus der falschen Aussage A (für P eingesetzt) die falsche Aussage A (für Q eingesetzt), was die vierte Zeile motiviert.

Wahrheitstafel der Bijunktion:

P	Q	$P \Leftrightarrow Q$
w	w	w
w	f	f
f	w	f
f	f	w

Die Wahrheitstafel der Bijunktion entspricht durchaus der umgangssprachlichen Bedeutung.

Mit Hilfe der Wahrheitstafeln können auch die Wahrheitswerte komplizierterer Aussagen getestet werden. Betrachten wir die Aussage

$$(A \vee B) \Rightarrow (C \wedge (\neg D)) ,$$

wobei A,B,C,D die Wahrheitswerte w,f,w,f haben sollen. Dann ist $A \vee B$ wahr, ebenso sind $\neg D$ und damit auch $C \wedge (\neg D)$

wahr. Also ist die gesamte Aussage wahr. Formal läßt sich unsere Überlegung schrittweise wie folgt schreiben:

$$
\begin{array}{ccccc}
(A \vee B) & \Rightarrow & (C \wedge (\neg D) \\
w \;\; f & & w \quad f \\
\quad w & & w \quad w \\
\quad w & & \quad w \\
\quad\quad w & &
\end{array}
$$

Als weiteres Beispiel betrachten wir die folgende Argumentation: " Wenn die Preise hoch sind, so sind die Löhne hoch. Preise sind hoch oder es existieren Preiskontrollen. Wenn es Preiskontrollen gibt, gibt es keine Inflation. Es herrscht Inflation. Daher sind die Löhne hoch." Angenommen, wir akzeptieren die ersten vier Sätze als wahre Aussagen. Müssen wir dann auch den letzten Satz als wahr akzeptieren ? Dazu formalisieren wir die Argumentation. Seien P , L , K bzw. I die Aussagen " Die Preise sind hoch " , " Die Löhne sind hoch " , " Es existieren Preiskontrollen " bzw. " Es herrscht Inflation ". Die Frage ist nun, ob aus der Wahrheit der Aussagen $P \Rightarrow L$, $P \vee K$, $K \Rightarrow \neg I$, I die Wahrheit der Aussage L folgt. Da I wahr ist, ist $\neg I$ falsch; da $K \Rightarrow \neg I$ wahr ist, ist K falsch; da $P \vee K$ wahr ist, ist P wahr; da $P \Rightarrow L$ wahr ist, ist L wahr.

1.3 Zur Verwendung der Bijunktion und des Gleichheitszeichens

Um Verwechslungen und Mißverständnissen vorzubeugen, sollen hier einige Bemerkungen über den Unterschied zwischen der Bijunktion " $\Leftrightarrow$ " und dem Gleichheitszeichen " = " gemacht werden.

Die Bijunktion wird n u r zwischen Aussagen und zwischen Aussageformen verwendet, nicht jedoch zwischen sonstigen mathematischen Objekten oder Elementen. Die Aussagen bzw. Aussageformen auf beiden Seiten des Bijunktionszeichens können durchaus verschieden sei, wie etwa in den folgenden

Beispielen:

$$\text{Der Mond ist rund} \iff \text{Moritz hat blonde Haare} \ ,$$

$$(\neg P \Rightarrow Q) \iff (P \vee Q) \ ,$$

$$(P \Rightarrow Q) \iff (Q \Rightarrow P) \ .$$

Selbstverständlich ist aber beispielsweise auch

$$(P \Rightarrow Q) \iff (P \Rightarrow Q)$$

eine Bijunktion.

Das Gleichheitszeichen hingegen kann zwischen beliebigen mathematischen und logischen Objekten auftreten - in der Bedeutung der Gleichheit der beiden verglichenen Objekte. Beispiele hierfür sind:

$$\pi = 3{,}141592... \ ,$$

$$2 + 2 = 16 : 4 \ ,$$

$$(P \Rightarrow Q) = (P \Rightarrow Q) \ .$$

Je nach der Art der mathematischen Objekte wird eine Erläuterung der verwendeten Gleichheit nötig sein oder sich aus dem Zusammenhang ergeben. Betrachtet man endliche Zeichenfolgen, gebildet aus Zahlen und den arithmetischen Zeichen +, -, ·, : , dann sind $2 + 2$ und $16 : 4$ verschieden. Betrachtet man jedoch die diesen Zeichenfolgen zugeordneten Zahlen, so sind $2 + 2$ und $16 : 4$ gleich.

Das Gleichheitszeichen kann seiner Bedeutung entsprechend nie als Ersatz für das Bijunktionszeichen stehen ! Im zuvor angegebenen dritten Beispiel für das Gleichheitszeichen soll ausgedrückt werden, daß auf beiden Seiten des Gleichheitszeichens dieselbe Aussageform $P \Rightarrow Q$ steht. Schreibt man jedoch

$$(P \Rightarrow Q) \iff (P \Rightarrow Q) \ ,$$

so ist dies wieder eine Aussageform - allerdings eine solche, die bei jeder Einsetzung von Aussagen für die Variablen den Wahrheitswert wahr ergibt. Dies ist "schwächer" als die Gleichheit der beiden Aussageformen auf den beiden Seiten der Bijunktion. So hat zum Beispiel auch die Aussageform

$$(\neg P \Rightarrow Q) \Leftrightarrow (P \vee Q)$$

die Eigenschaft, bei jeder Einsetzung von Aussagen für die Variablen den Wahrheitswert wahr zu liefern, selbstverständlich gilt jedoch n i c h t $(\neg P \Rightarrow Q) = (P \vee Q)$. Auf derartige Aussageformen, sogenannte Tautologien gehen wir im nächsten Abschnitt genauer ein.

Für den Umgang mit dem Gleichheitszeichen ergeben sich die folgenden Eigenschaften:

1) R e f l e x i v i t ä t : Für alle mathematischen (und logischen) Objekte A gilt $A = A$;
2) S y m m e t r i e : Gilt $A = B$, so gilt auch $B = A$;
3) T r a n s i t i v i t ä t : Gelten $A = B$ und $B = C$, so gilt auch $A = C$;
4) E i n s e t z u n g : Gilt $A = B$ und ist P(A) eine wahre mathematische Aussage (die unter Verwendung von A gebildet wird), so ist auch P(B) eine wahre Aussage.

Die ersten drei Eigenschaften sind die einer Äquivalenzrelation (siehe III.2.1). Die vierte Eigenschaft besagt, daß im Falle $A = B$ an allen Stellen, an denen A auftritt, A durch B ersetzt werden kann.

1.4 Tautologien, ihre Bedeutung und Bestimmung

Im vorhergehenden Abschnitt haben wir zwei Aussageformen,

$$(P \Rightarrow Q) \Leftrightarrow (P \Rightarrow Q) \quad , \quad (\neg P \Rightarrow Q) \Leftrightarrow (P \vee Q)$$

kennen gelernt, die bei jeder Einsetzung von Aussagen für die Variablen eine wahre Aussage ergeben.

Es soll ein weiteres Beispiel für derartige Aussageformen betrachtet werden. In 1.2 wurde aus der Tatsache, daß P und $P \Rightarrow L$ wahre Aussagen sind, darauf geschlossen, daß L wahr ist. Also wurde ein Schluß der Form

$$(P \wedge (P \Rightarrow L)) \Rightarrow L$$

verwendet.

Betrachten wir die entsprechende Aussageform jetzt mit Aussagevariablen P und Q und bestimmen wir alle Wahrheitswerte bei Einsetzung von Aussagen für die Variablen. Die Berechnung kann nach dem in 1.2 angegebenen Schema durchgeführt werden, wobei noch beispielsweise statt

$$\begin{array}{llllll} (P & \wedge & (P & \Rightarrow & Q)) & \Rightarrow Q \\ w & & w & & f & f \\ w & & & f & & f \\ & f & & & & f \end{array}$$

$$w$$

durch Zusammenschieben der Zeilen

$$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$$
$$w\ f\ w\ f\ \ f\ \ \ w\ \ f$$

geschrieben werden soll. Dann ergibt sich die folgende Tabelle

P	Q	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
w	w	w w w w w w w
w	f	w f w f f w f
f	w	f f f w w w w
f	f	f f f w f w f

Die vorletzte Spalte zeigt, daß die hier betrachtete Aussageform immer den Wahrheitswert w erhält, gleichgültig ob man für P und Q wahre oder falsche Aussagen einsetzt. Eine solche Aussageform, die bei jeder Einsetzung von Aussagen in die Variablen eine wahre Aussage ergibt, nennt man eine T a u t o l o g i e oder ein G e s e t z d e r A u s s a g e n l o g i k . Die zuletzt besprochene Tautologie $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ wird auch G e s e t z z u m m o d u s p o n e n s genannt.

Ebenso wie im Falle dieser Tautologie können viele weitere Aussageformen als Tautologien bestätigt werden. Der Leser möge sich durch Beispiele die Bedeutung der folgenden Tautologien klarmachen und sich davon überzeugen, daß auch der "gesunde Menschenverstand" sie als allgemeingültig

erkennt. Im Zweifelsfall kann er eine Berechnung nach dem angegebenen Schema durchführen.

Bei den folgenden Formulierungen beachte man, daß Klammern im Sinne unserer Ausführungen am Ende von 1.1 so weit wie möglich vermieden werden.

T a u t o l o g i s c h e S u b j u n k t i o n e n

1)	$P \wedge (P \Rightarrow Q) \Rightarrow Q$	Gesetz zum modus ponens
2)	$\neg Q \wedge (P \Rightarrow Q) \Rightarrow \neg P$	G.z. modus tollens
3)	$\neg P \wedge (P \vee Q) \Rightarrow Q$	
4)	$P \Rightarrow (Q \Rightarrow P \wedge Q)$	
5)	$P \wedge Q \Rightarrow P$	G.z. Konjunktionsschluß
6)	$P \Rightarrow P \vee Q$	G.z. Disjunktionsschluß
7)	$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$	G.z. modus barbara
8)	$(P \wedge Q \Rightarrow R) \Rightarrow (P \Rightarrow (Q \Rightarrow R))$	
9)	$(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \wedge Q \Rightarrow R)$	
10)	$(P \Rightarrow Q \wedge \neg Q) \Rightarrow \neg P$	
11)	$(P \Rightarrow Q) \Rightarrow (P \vee R \Rightarrow Q \vee R)$	
12)	$(P \Leftrightarrow P_1) \wedge (Q \Leftrightarrow Q_1) \Rightarrow (P \vee Q \Leftrightarrow P_1 \vee Q_1)$	
13)	$(P \Rightarrow Q) \Rightarrow (P \wedge R \Rightarrow Q \wedge R)$	
14)	$(P \Leftrightarrow P_1) \wedge (Q \Leftrightarrow Q_1) \Rightarrow (P \wedge Q \Leftrightarrow P_1 \wedge Q_1)$	
15)	$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$	
16)	$(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R) \Rightarrow (P \Leftrightarrow R)$	

T a u t o l o g i s c h e B i j u n k t i o n e n

17)	$P \Leftrightarrow P$
18)	$(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$
19)	$(P \Rightarrow R) \wedge (Q \Rightarrow R) \Leftrightarrow (P \vee Q \Rightarrow R)$
20)	$(P \Rightarrow Q) \wedge (P \Rightarrow R) \Leftrightarrow (P \Rightarrow Q \wedge R)$

21) $P \vee Q \Longleftrightarrow Q \vee P$ — Kommutativgesetze

21') $P \wedge Q \Longleftrightarrow Q \wedge P$

22) $(P \vee Q) \vee R \Longleftrightarrow P \vee (Q \vee R)$ — Assoziativgesetze

22') $(P \wedge Q) \wedge R = P \wedge (Q \wedge R)$

23) $P \vee (Q \wedge R) \Longleftrightarrow (P \vee Q) \wedge (P \vee R)$ — Distributivgesetze

23') $P \wedge (Q \vee R) \Longleftrightarrow (P \wedge Q) \vee (P \wedge R)$

24) $P \vee P \Longleftrightarrow P$ — Idempotenzgesetze

24') $P \wedge P \Longleftrightarrow P$

25) $P \vee (P \wedge Q) \Longleftrightarrow P$ — Absorptionsgesetze

25') $P \wedge (P \vee Q) \Longleftrightarrow P$

26) $(P \vee \neg P) \wedge Q \Longleftrightarrow Q$

27) $\neg (P \vee \neg P) \vee Q \Longleftrightarrow Q$

Tautologien zur Ersetzung der Junktoren

28) $(P \Longrightarrow Q) \Longleftrightarrow \neg P \vee Q$

29) $(P \Longrightarrow Q) \Longleftrightarrow \neg (P \wedge \neg Q)$

30) $(P \vee Q) \Longleftrightarrow (\neg P \Longrightarrow Q)$

31) $(P \vee Q) \Longleftrightarrow \neg (\neg P \wedge \neg Q)$

32) $(P \wedge Q) \Longleftrightarrow \neg (P \Longrightarrow \neg Q)$

33) $(P \wedge Q) \Longleftrightarrow \neg (\neg P \vee \neg Q)$

34) $(P \Longleftrightarrow Q) \Longleftrightarrow ((P \Longrightarrow Q) \wedge (Q \Longrightarrow P))$

Tautologien zur Verneinung

35) $\neg \neg P \Longleftrightarrow P$ — Satz von der doppelten Verneinung

36) $\neg (P \vee Q) \Longleftrightarrow \neg P \wedge \neg Q$ — Gesetze von De Morgan

36') $\neg (P \wedge Q) \Longleftrightarrow \neg P \vee \neg Q$

37) $\neg (P \wedge Q) \Longleftrightarrow (P \Longrightarrow \neg Q)$

38) $\neg (P \Longrightarrow Q) \Longleftrightarrow P \wedge \neg Q$

39) $\neg (P \Longleftrightarrow Q) \Longleftrightarrow (P \Longleftrightarrow \neg Q)$

Tautologien für die Technik des indirekten Beweises

40)	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$	Kontrapositionsgesetz
41)	$(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q \Rightarrow \neg P)$	
42)	$(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q \Rightarrow Q)$	
43)	$(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q \Rightarrow R \wedge \neg R)$	
44)	$P \vee \neg P$	Satz vom ausgeschlossenen Dritten
45)	$\neg (P \wedge \neg P)$	Satz vom Widerspruch

1.5 Arithmetische Berechnung von Tautologien

Tautologien können, statt mit Hilfe der Wahrheitstafeln, auch auf eine rein arithmetische Weise nachgeprüft werden. Wir wollen hier nur die entsprechende Rechnung angeben, ohne auf die Begründung einzugehen, die für diese Darstellung zu umfangreich wäre. Die Verknüpfungen werden auf folgende Art dargestellt:

Aussageform	Arithmetische Darstellung
$\neg P$	$1 + P$
$P \wedge Q$	$P + Q + P \cdot Q$
$P \vee Q$	$P \cdot Q$
$P \Rightarrow Q$	$(1 + P) \cdot Q$
$P \Leftrightarrow Q$	$P + Q$

Die arithmetischen Werte komplizierterer Formeln können nach den üblichen Rechenregeln für Addition und Multiplikation von Zahlen umgerechnet werden, nur daß jetzt zusätzlich die folgenden Regeln gelten:

$$1 + 1 = 0 \quad , \quad P + P = 0 \quad , \quad P \cdot P = P^2 = P \quad ,$$

wobei P eine beliebige Aussagevariable ist. (Rechnen in einem Booleschen Ring; siehe dazu IV.3.6.1). Es gilt dann die folgende Behauptung :

Der arithmetische Wert einer Aussageform ist genau dann gleich 0 , wenn die Aussageform eine Tautologie ist.

Zum Beispiel ist für $P \wedge (P \Rightarrow Q) \Rightarrow Q$ der arithmetische Wert

$$
\begin{aligned}
&(1 + P + (1 + P)\cdot Q + P\cdot(1 + P)\cdot Q)\cdot Q \\
&= (1 + P + Q + P\cdot Q + P\cdot Q + P\cdot P\cdot Q)\cdot Q \\
&= (1 + P + Q + (P + P)\cdot Q + P\cdot Q)\cdot Q \\
&= (1 + P + Q + P\cdot Q)\cdot Q = Q + P\cdot Q + Q\cdot Q + P\cdot Q\cdot Q \\
&= Q + P\cdot Q + Q + P\cdot Q = (Q + Q) + (P + P)\cdot Q = 0 .
\end{aligned}
$$

§ 2 Prädikatenlogik

2.1 Prädikate

Die zuvor angegebenen Tautologien sind in dem Sinne wahr, daß sie bei beliebiger Einsetzung von Aussagen für die Aussagevariablen wahre Aussagen ergeben. Häufig beschränkt man jedoch die Auswahl der einzusetzenden Aussagen auf eine Weise, die durch das folgende Beispiel erläutert werden soll. Für die Aussagevariable P setze man nur Aussagen der Form "x ist eine ganze Zahl" ein, wie zum Beispiel "2 ist eine ganze Zahl", "-7 ist eine ganze Zahl", "5/4 ist eine ganze Zahl" oder "Die Sonne ist eine ganze Zahl". Dabei soll es also zugelassen werden, daß für x beliebige Subjekte eingesetzt werden. Da man x von vornherein nicht spezifizieren möchte, betrachtet man x als Variable und bezeichnet "x ist eine ganze Zahl" als P r ä d i k a t in der Variablen x .

Weitere Beispiele für eine solche Situation sind: "$y^2 = 4 \wedge y > 0$" sowie "X ist ein Bruder von Y". Die Zeichen x,y,X,Y, die in diesem Zusammenhang verwendet worden sind, werden S u b j e k t v a r i a b l e n genannt, in die beliebige Subjekte eingesetzt werden (,wobei Subjekte nicht im grammatikalischen Sinne zu verstehen sind). Allgemein soll ein P r ä d i k a t $P(x_1, \ldots, x_n)$ in den Subjektvariablen $x_1, \ldots, x_n$ ein Ausdruck sein, der bei beliebiger Einsetzung von Subjekten $a_1, \ldots, a_n$ für $x_1, \ldots, x_n$ eine Aussage $P(a_1, \ldots, a_n)$ ergibt (,die entweder wahr oder falsch ist).

Selbstverständlich kann man gewisse Subjektvariablen durch andere Subjektvariablen ersetzen und erhält dann wieder Prädikate. Beim Einsetzen muß nur konsequent eine Subjektvariable an allen Stellen, an denen sie vorkommt, durch dieselbe Subjektvariable ersetzt werden.

Ebenso wie zwischen Aussageformen kann man selbstverständlich auch logische Verknüpfungen zwischen Prädikaten

ausführen und erhält wieder Prädikate. Die Tautologien geben uns nun die Möglichkeit, auch mit den Prädikaten logische Schlüsse durchzuführen, ohne daß man auf die Wahrheitswerte achten muß, die die Prädikate beim Einsetzen von Subjekten annehmen. So ist zum Beispiel immer wahr

$$(x \text{ ist ein Engländer}) \wedge ((x \text{ ist ein Engländer}) \Longrightarrow (x \text{ ist ein Mensch})) \Longrightarrow (x \text{ ist ein Mensch}) ,$$

unabhängig davon, ob wir $x = \text{John}$ oder $x = \text{Sonne}$ einsetzen. Das vorstehende Prädikat ist aus dem Gesetz zum modus ponens hervorgegangen.

Die wichtigste Eigenschaft der Tautologien liegt in dem folgenden Zusammenhang. Entsteht

$$P(x_1, \ldots, x_n) \Longrightarrow Q(x_1, \ldots, x_n)$$

aus einer Tautologie, indem man darin alle Aussagevariablen durch Prädikate ersetzt, so daß also auch $P(x_1, \ldots, x_n)$ und $Q(x_1, \ldots, x_n)$ Prädikate sind, und sind $a_1, \ldots, a_n$ Subjektvariablen , so daß $P(a_1, \ldots, a_n)$ wahr ist, so ist auch $Q(a_1, \ldots, a_n)$ wahr. Das ergibt sich aus der Tautologie und der Wahrheitstafel für die Subjunktion. Man kann also von $P(x_1, \ldots, x_n)$ auf $Q(x_1, \ldots, x_n)$ "schließen". Ähnliches gilt für aus Tautologien entstandene Prädikate der Form $P(x_1, \ldots, x_n) \Longleftrightarrow Q(x_1, \ldots, x_n)$.

Betrachten wir ein weiteres Beispiel. Aus dem Gesetz zum modus tollens ergibt sich

$$(x \text{ ist keine rationale Zahl}) \wedge ((x \text{ ist eine ganze Zahl}) \Longrightarrow (x \text{ ist eine rationale Z.})) \Longrightarrow (x \text{ ist keine ganze Zahl}) .$$

Da wir von der Wahrheit von

$$(x \text{ ist eine ganze Zahl}) \Longrightarrow (x \text{ ist eine rationale Z.})$$

für jedes x überzeugt sind, ist also die linke Seite dieser Subjunktion wahr, wenn wir $x = \sqrt{2}$ setzen. Dann ist aber auch "($\sqrt{2}$ ist keine ganze Zahl)" wahr.

2.2 Prädikate und Quantoren

Wie schon angegeben, erhält man aus dem Prädikat P(x) mit der einzigen Subjektvariablen x durch Einsetzen eines Subjektes a für x die Aussage P(a). Es gibt aber auch noch einen anderen Weg, um aus Prädikaten Aussagen zu erhalten, nämlich durch die Q u a n t o r e n . Wir verwenden den A l l q u a n t o r "$\forall x$" , umgangssprachlich ausgedrückt durch "Für alle x ..." oder "Für jedes x ..." , und den E x i s t e n z q u a n t o r "$\exists x$" , umgangssprachlich ausgedrückt durch "Es gibt ein x ..." oder "Es existiert (mindestens) ein x ...". (Zur Auswahl der Subjekte x siehe auch 2.4).

Ist P(x) ein Prädikat, so sind $\forall x\,[P(x)]$ und $\exists x\,[P(x)]$ Aussagen; im ersten Falle handelt es sich um die Aussage "Für alle x gilt P(x)", die wahr oder falsch sein kann, im zweiten Falle um die Aussage "Es gibt (mindestens) ein x, so daß P(x) gilt", die ebenfalls wahr oder falsch sein kann. Ist $P(x_1,\ldots,x_n)$ ein n-stelliges Prädikat, das heißt ein Prädikat mit n verschiedenen Subjektvariablen, so sind $\forall x_1\,[P(x_1,\ldots x_n)]$ bzw. $\exists x_1\,[P(x_1,\ldots,x_n)]$ (n-1)-stellige Prädikate in den Subjektvariablen $x_2,\ldots x_n$. Für die Subjektvariablen $x_2,\ldots,x_n$ darf man noch beliebige Subjekte $a_2,\ldots,a_n$ einsetzen, um Aussagen der Form $\forall x_1\,[P(x_1,a_2,\ldots,a_n)]$ bzw. $\exists x_1\,[P(x_1,a_2,\ldots,a_n)]$ zu erhalten. Für x_1 darf natürlich kein Subjekt eingesetzt werden, da sonst der Quantor $\forall x_1$ bzw. $\exists x_1$ sinnlos wäre. In $\forall x_1\,[P(x_1,x_2,\ldots,x_n)]$ bzw. $\exists x_1\,[P(x_1,x_2,\ldots,x_n)]$ werden $x_2,\ldots,x_n$ auch als f r e i e V a r i a b l e n bezeichnet, während x_1 g e b u n d e n e V a r i a b l e heißt. Selbstverständlich können in einem Prädikat auch mehrere gebundene Variablen vorkommen.

Einige Beispiele mögen den Gebrauch der Quantoren veranschaulichen. Die Aussage "Jede ganze Zahl ist eine rationale Zahl" läßt sich auch wie folgt ausdrücken:"Für jedes x gilt: Wenn x eine ganze Zahl ist,dann ist x eine rationale Zahl". Führen wir nun für "x ist eine ganze Zahl" das Prädikat Z(x) und für "x ist eine rationale Zahl" das

Prädikat $Q(x)$ ein, so läßt sich diese Aussage wie folgt darstellen:

$$\forall x \, [Z(x) \Rightarrow Q(x)] \; .$$

Ähnlich läßt sich die Aussage "Es gibt rationale Zahlen, die ganze Zahlen sind" in der Form

$$\exists x \, [Q(x) \wedge Z(x)]$$

darstellen. Man beachte daß die Aussage so zu verstehen ist: "Es gibt ein x, so daß x eine rationale Zahl ist und außerdem noch eine ganze Zahl ist".

An dieser Stelle sei der Leser besonders davor gewarnt, die Aussage $\exists x \, [Q(x) \wedge Z(x)]$ mit der Aussage $\exists x \, [Q(x) \Rightarrow Z(x)]$ zu verwechseln. Am besten wird das an den Prädikaten "x ist eine ganze Zahl" = $Z(x)$ und "x ist eine irrationale Zahl" = $I(x)$ klar. Die Aussage $\exists x \, [Z(x) \wedge I(x)]$, also "es gibt eine ganze Zahl, die irrational ist", ist sicher falsch. Jedoch ist die Aussage $\exists x \, [Z(x) \Rightarrow I(x)]$ wahr, denn sie bedeutet "es gibt ein x, so daß x irrationale Zahl ist, falls x ganze Zahl ist". Wir können solche x angeben wie zum Beispiel $x = 1/2$ oder $x = \sqrt{2}$. Beide Zahlen 1/2 und $\sqrt{2}$ sind nicht ganz. Da "1/2 ist eine ganze Zahl" falsch ist, ist nach der Wahrheitstafel für die Subjunktion $Z(1/2) \Rightarrow I(1/2)$ wahr. Das gleiche gilt für $Z(\sqrt{2}) \Rightarrow I(\sqrt{2})$. Man beachte, daß in der ersten Subjunktion $I(1/2)$ falsch und in der zweiten Subjunktion $I(\sqrt{2})$ wahr ist.

Nach diesen einführenden Überlegungen müssen wir noch etwas genauer auf den Wahrheitswert von $\forall x \, [P(x)]$ und $\exists x \, [P(x)]$ eingehen. $\forall x \, [P(x)]$ ist wahr, wenn für jedes Subjekt a die Aussage $P(a)$ wahr ist. Gibt es mindestens ein Subjekt a, so daß $P(a)$ falsch ist, so soll $\forall x \, [P(x)]$ den Wahrheitswert falsch haben. $\exists x \, [P(x)]$ hat den Wahrheitswert wahr, wenn es mindestens ein Subjekt a gibt, so daß $P(a)$ wahr ist. Ist für alle Subjekte a die Aussage $P(a)$ falsch, so soll $\exists x \, [P(x)]$ falsch sein.

Nach dieser Definition der Wahrheitswerte erkennt man, daß der Allquantor $\forall$ eine Verallgemeinerung der Konjunktion $\wedge$ ist. Daher kommt in der Literatur auch das Symbol $\bigwedge$ an

Stelle von $\forall$ vor. Beispielsweise ist $P(a_1) \wedge P(a_2) \wedge P(a_3)$ genau dann wahr, wenn $P(a_1)$ und $P(a_2)$ und $P(a_3)$ alle wahr sind. $\forall x [P(x)]$ ist genau dann wahr, wenn für alle Subjekte a die Aussage P(a) wahr ist. Schränkt man die Möglichkeit der Subjektauswahl auf a_1, a_2 und a_3 ein, so erhält man also die Konjunktion $P(a_1) \wedge P(a_2) \wedge P(a_3)$. Ähnlich ist der Existenzquantor eine Verallgemeinerung der Disjunktion, wie man sich an $\exists x [P(x)]$ beziehungsweise $P(a_1) \vee P(a_2) \vee P(a_3)$ klar machen kann. $\exists x [P(x)]$ ist nämlich genau dann wahr, wenn für mindestens ein a die Aussage P(a) wahr ist. Und $P(a_1) \vee P(a_2) \vee P(a_3)$ ist genau dann wahr, wenn für mindestens eines der a_1, a_2 und a_3 die Aussage $P(a_i)$ wahr ist. Neben dem Symbol $\exists$ wird daher in der Literatur auch $\bigvee$ verwendet.

Die folgenden Bemerkungen über die Umbenennung von Subjektvariablen ist stets zu beachten. Zunächst ist es offenbar gleichgültig, ob man $\forall x [P(x)]$ oder $\forall y [P(y)]$ schreibt. Gebundene Variablen können in dieser Weise umbenannt werden. Das gilt auch, wenn die gebundenen Variablen mehrfach mit verschiedenen Bindungen vorkommen. So haben $\exists x [P(x)] \wedge \forall x [Q(x)]$ und $\exists y [P(y)] \wedge \forall y [Q(y)]$ und $\exists y [P(y)] \wedge \forall x [Q(x)]$ alle den gleichen Wahrheitswert, wie unmittelbar aus der Definition der Quantoren folgt.

Bei der Umbenennung von freien Variablen ist Vorsicht geboten. Zum Beispiel ist $(x \leq 7 \wedge 8 \leq y)$ etwas anderes als $(y \leq 7 \wedge 8 \leq y)$, denn im ersten Fall ist das Prädikat für $x = 7$ und $y = 8$ wahr, während im zweiten Fall kein Subjekt a existiert, das das Prädikat erfüllt. Wir merken uns daher, daß die freie Variable x durch die Variable y nur ersetzt werden kann, wenn y nicht schon in dem Prädikat als freie Variable vorkommt. Diese Ersetzung darf auch dann nicht vorgenommen werden, wenn x im Wirkungsbereich eines Quantors für y liegt, da dann die freie Variable x durch die Ersetzung verschwinden würde und für y neue Bedingungen hinzukommen könnten.

In §1 haben wir schon Regeln eingeführt, um umfangreiche

Klammerungen zu vermeiden. In diese Regeln sind die Quantoren noch einzubeziehen. Zunächst sind Quantoren an das in $[\cdots]$ stehende, direkt folgende Prädikat gebunden. Treten mehrere Quantoren hintereinander auf, so sind sie in der Reihenfolge von rechts nach links zu berücksichtigen. So wird zum Beisoiel

$$\forall x\, \exists y\, \forall z\, [P(x,y,z) \Longrightarrow Q(x,z)]$$

statt ausführlich

$$\forall x [\exists y [\forall z [P(x,y,z) \Longrightarrow Q(x,y)]]]$$

geschrieben.

2.3 Quantoren und Junktoren, allgemeingültige Prädikate

Es sollen jetzt Regeln über Beziehungen zwischen den Quantoren und den Junktoren angegeben werden. Wir formulieren diese Beziehungen als allgemeingültige Prädikate. Dabei heißt ein Prädikat $P(x_1,\ldots,x_n)$ a l l g e m e i n g ü l t i g e s P r ä d i k a t , falls für beliebige Subjekte $a_1,\ldots,a_n$ die Aussage $P(a_1,\ldots,a_n)$ wahr ist.

Allgemeingültige Prädikate für die
V e r t a u s c h u n g v o n Q u a n t o r e n

1) $\forall x[\forall y [P(x,y,z)]] \Longleftrightarrow \forall y[\forall x [P(x,y,z)]]$

2) $\exists x[\exists y [P(x,y,z)]] \Longleftrightarrow \exists y[\exists x [P(x,y,z)]]$

3) $\exists x[\forall y [P(x,y,z)]] \Longrightarrow \forall y[\exists x [P(x,y,z)]]$

In diesen Formeln kann z eine oder mehrere freie Variablen bedeuten oder aber, daß keine freie Variable vorkommt. Man beachte ferner, daß sich durch Umkehrung des Pfeiles in 3) kein allgemeingültiges Prädikat ergibt. So ist zum Beispiel

$\forall y[\exists x [x$ ist rationale Zahl $\wedge$ (y ist ganze Zahl $\Longrightarrow 2x = y)]]$

eine wahre Aussage; für eine ganze Zahl y sei $x = \frac{1}{2}y$, sonst etwa $x = 1$. Hingegen ist die folgende Aussage falsch

$\exists x[\forall y [x$ ist rationale Zahl $\wedge$ (y ist ganze Zahl $\Longrightarrow 2x = y)]]$,

denn es kann keine feste rationale Zahl a geben, so daß

2a = y für alle ganzen Zahlen y gilt.

Um beispielsweise die Allgemeingültigkeit von 3) zu zeigen, nehmen wir an, daß für $z = c$ die linke Seite von 3), also $\exists x[\forall y[P(x,y,c)]]$ wahr ist. Dann gibt es also ein a, so daß $\forall y[P(a,y,c)]$ wahr ist. Für jedes Subjekt b ist daher P(a,b,c) wahr. Dann ist offenbar auch für jedes Subjekt b die Aussage $\exists x[P(x,b,c)]$ wahr, also ist $\forall y[\exists x[P(x,y,c)]]$ wahr. Folglich ist auch

$$\exists x[\forall y[P(x,y,c)]] \Longrightarrow \forall y[\exists x[P(x,y,c)]]$$

wahr. Ist hingegen $\exists x[\forall y[P(x,y,c)]]$ falsch, so ist vorstehende Subjunktion ebenfalls wahr. Damit ist gezeigt, daß 3) allgemeingültig ist. Die Allgemeingültigkeit von 1) und 2) sowie der folgenden Prädikate kann man ähnlich beweisen.

Allgemeingültige Prädikate für die
Verneinung von Quantoren

4) $\neg(\forall x[P(x,z)]) \Longleftrightarrow \exists x[\neg P(x,z)]$

5) $\neg(\exists x[P(x,z)]) \Longleftrightarrow \forall x[\neg P(x,z)]$

Als Beispiel zur Verneinung von Quantoren negieren wir die Aussage

$$\forall\varepsilon[P(\varepsilon) \Longrightarrow \exists\delta[P(\delta) \wedge \forall x[Q(\delta,x) \Longrightarrow R(\varepsilon,x)]]]$$

Die Negation hiervon kann man mit Hilfe der allgemeingültigen Prädikate 4) und 5) sowie der Tautologien 38), 36) und 28) in die Form

$$\exists\varepsilon[P(\varepsilon) \wedge \forall\delta[P(\delta) \Longrightarrow \exists x[Q(\delta,x) \wedge \neg R(\varepsilon,x)]]]$$

bringen, wie der Leser zur Übung nachprüfen möge. Wählt man die folgenden Prädikate:

$P(\varepsilon)$ = " ε ist eine reelle Zahl und $\varepsilon > 0$ " ,

$Q(\delta,x)$ = " δ und x sind reelle Zahlen und $|x - x_0| < \delta$ " ,

$R(\varepsilon,x)$ = " ε und x sind reelle Zahlen und $|f(x) - f(x_0)| < \varepsilon$ " ,

wobei x_0 eine feste reelle Zahl und $f : \mathbb{R} \longrightarrow \mathbb{R}$ eine

Abbildung sind, dann ist die erste Aussage die Definition der Stetigkeit der Abbildung f im Punkt x_0 und die zweite ihre Negation, das heißt, ihre Unstetigkeit im Punkt x_0.

Hier wird nochmals klar, warum die Aussage "Es gibt rationale Zahlen, die ganze Zahlen sind" in der Form $\exists x[Q(x) \wedge Z(x)]$ geschrieben wird. Die Negation ist nämlich: "Es gibt keine rationale Zahl, die ganze Zahl ist" oder "Für alle x gilt: Ist x eine rationale Zahl, so ist x keine ganze Zahl", formal also $\forall x\,[Q(x) \Rightarrow \neg\, Z(x)]$. Verneinen wir diese Aussage nochmals, um die ursprüngliche Aussage zu erhalten, so gilt

$$(\neg\,(\forall x\,[\,Q(x) \Rightarrow \neg\, Z(x)]\,) \Longleftrightarrow (\exists x[\neg\,(Q(x) \Rightarrow \neg\, Z(x))])$$
$$\Longleftrightarrow (\exists x[Q(x) \wedge \neg\,\neg\, Z(x)]) \Longleftrightarrow (\exists x[Q(x) \wedge Z(x)])\ .$$

Die Verneinungsformeln 4) und 5) ergeben auch die Möglichkeit, einen der beiden Quantoren durch den anderen zu ersetzen:

$$\forall x\,[P(x,z)] \Longleftrightarrow \neg\,(\exists x[\neg\, P(x,z)])\ ,$$
$$\exists x\,[P(x,z)] \Longleftrightarrow \neg\,(\forall x[\neg\, P(x,z)])\ .$$

Allgemeingültige Prädikate für
Quantoren und Junktoren

6) $\forall x\,[P(x,z) \wedge Q(x,z)] \Longleftrightarrow (\forall x\,[P(x,z)] \wedge \forall x\,[Q(x,z)])$

7) $\exists x\,[P(x,z) \vee Q(x,z)] \Longleftrightarrow (\exists x\,[P(x,z)] \vee \exists x\,[Q(x,z)])$

8) $\forall x\,[P(z) \wedge Q(x,z)] \Longleftrightarrow (P(z) \wedge \forall x\,[Q(x,z)])$

9) $\exists x\,[P(z) \vee Q(x,z)] \Longleftrightarrow (P(z) \vee \exists x\,[Q(x,z)])$

10) $\forall x\,[P(z) \vee Q(x,z)] \Longleftrightarrow (P(z) \vee \forall x\,[Q(x,z)])$

11) $\exists x\,[P(z) \wedge Q(x,z)] \Longleftrightarrow (P(z) \wedge \exists x\,[Q(x,z)])$

12) $(\forall x\,[P(x,z)] \vee \forall x\,[Q(x,z)]) \Rightarrow \forall x\,[P(x,z) \vee Q(x,z)]$

13) $\exists x\,[P(x,z) \wedge Q(x,z)] \Rightarrow (\exists x\,[P(x,z)] \wedge \exists x\,[Q(x,z)])$

14) $\exists x\,[P(x,z) \Rightarrow Q(x,z)] \Longleftrightarrow (\forall x\,[P(x,z)] \Rightarrow \exists x\,[Q(x,z)])$

15) $(\exists x\,[P(x,z)] \Rightarrow \forall x\,[Q(x,z)]) \Rightarrow \forall x\,[P(x,z) \Rightarrow Q(x,z)]$

2.4 Zur Auswahl der Subjekte, Spezialisierung und Verallgemeinerung

Häufig interessieren uns in ganz bestimmten Zusammenhängen nur gewisse Subjekte, aber keinesfalls alle möglichen Subjekte. Wenn man über die Eigenschaften der ganzen Zahlen spricht, sind Subjekte wie "Sonne" , "Seele" oder "Salat" nicht von Interesse. Deshalb schränkt man in diesem Zusammenhang den Bereich der zugelassenen Subjekte von vorn herein durch Angabe einer Menge M (siehe dazu Kapitel II) ein, aus der nur Subjekte zulässig sind. Statt $\forall x\,[P(x,z)]$ schreibt man also $\forall x \in M\,[P(x,z)]$, was dasselbe bedeuten soll wie $\forall x\,[x \in M \Rightarrow P(x,z)]$. Entsprechend wird statt $\exists x\,[P(x,z)]$ mit der Beschränkung $x \in M$ auch $\exists x \in M\,[P(x,z)]$ geschrieben, was dasselbe bedeutet wie $\exists x\,[x \in M \wedge P(x,z)]$. So ist zum Beispiel $\exists x \in \mathbb{Q}\,[2x = 1]$ eine wahre Aussage, weil $2x = 1$ die Lösung $1/2 \in \mathbb{Q}$ (= Menge der rationalen Zahlen) hat. Jedoch ist $\exists x \in \mathbb{Z}\,[2x = 1]$ falsch, weil $2x = 1$ keine Lösung in $\mathbb{Z}$ (= Menge der ganzen Zahlen) besitzt.

Bei mathematischen Beweisen, vor allem, wenn sie nicht durchgehend mit den logischen Zeichen formuliert werden, ist nicht immer ganz leicht zu erkennen, welcher Teil der Voraussetzung an welcher Stelle verwendet wird. Obwohl der Mathematiker bei der Formulierung seiner Sätze auf möglichst geringe Voraussetzungen Wert legt, kommt es doch vor, daß für einen Beweis nur ein Teil aller gegebenen Voraussetzungen verwendet wird. Man merke sich: Besteht eine Aussage aus mehreren (durch die Konjunktion verbundenen) Teilaussagen, und ist die Aussage wahr, dann ist auch jede Teilaussage wahr. Besonders die Spezialisierung von "All-Aussagen" bringt immer wieder Verständnisschwierigkeiten mit sich. Wenn als Voraussetzung etwa gegeben ist $\forall x\,[P(x)]$ und im Beweis an einer Stelle ein x_0 auftritt, so ist $P(x_0)$ wahr und kann in der Folge im Beweis verwendet werden. Soll jedoch $\forall x\,[P(x)]$ bewiesen werden, so genügt es nicht, für ein spezielles x_0 zu zeigen, daß $P(x_0)$ wahr ist. $P(x_0)$ ist zwar für die allgemeingültige Aussage $\forall x\,[P(x)]$ ein Beispiel, das eventuell zu einer

Beweisidee anregen kann, doch nicht mehr. Merke: Eine "All-Aussage" in der Voraussetzung kann spezialisiert werden, eine "All-Aussage" in der Behauptung wird nicht durch einen Spezialfall bewiesen.

II. Kapitel: Grundbegriffe der Mengenlehre

§ 1 Axiome der Mengenlehre

1.1 Einleitung

Als Sprache zur Formulierung mathematischer Begriffe und Zusammenhänge wird heute allgemein die Sprache der Mengenlehre benutzt. Es gilt daher zunächst, die Grundbegriffe der Mengenlehre in entsprechendem Umfang zu entwickeln. Das bedeutet, daß wir nur die einfachsten Anfangsgründe der Mengenlehre darstellen.

Mit der Entwicklung der Mengenlehre sind vor allem die Namen George B o o l e (1815 - 1864) und Georg C a n t o r (1845 - 1918) verbunden. G.Boole stellte als erster die algebraischen Operationen mit Mengen - Durchschnitt, Vereinigung und Komplementärmenge - heraus, während G.Cantor als der eigentliche Begründer der Mengenlehre anzusehen ist. Er entwickelte bereits wesentliche Teile der Theorie der Kardinal- und Ordinalzahlen. Zur weiteren Verbreitung der Mengenlehre bis zum heutigen Stand, wo die Mengenlehre zur mathematischen Allgemeinbildung eines jeden Mathematikers gehört, hat vor allem das Buch von F. H a u s d o r f f "Grundzüge der Mengenlehre" , 1.Auflage 1914 , beigetragen.

Von G.Cantor stammt die folgende inhaltliche "Definition" einer Menge:

> Eine Menge M ist die Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen".

Daß es sich dabei tatsächlich nicht um eine mathematische Definition handelt, ist klar, denn die darin vorkommenden Begriffe sind selbst undefiniert. Dennoch ist diese Formulierung geeignet, eine gute intuitive Vorstellung vom Begriff der Menge zu geben.

Wir werden hier auf eine explizite Definition des Begriffes einer Menge überhaupt verzichten (müssen !) und uns mit einer impliziten Definition begnügen. Implizite Definitionen sind vom synthetischen Aufbau der Geometrie - zum Teil bereits aus der Schule - wohlbekannt. Auch hier wird nicht definiert, was etwa Punkte, Geraden und Ebenen sind, sondern es werden nur die Beziehungen definiert, die zwischen ihnen bestehen sollen. Zum Beispiel wird gefordert, daß durch zwei verschiedene Punkte genau eine Gerade bestimmt sein soll, die diese Punkte enthält, und daß zwei verschiedene Geraden (im affinen Falle) entweder keinen oder genau einen gemeinamen Punkt enthalten sollen. Durch derartige axiomatische Bedingungen werden Punkte und Geraden implizit, aber in Übereinstimmung mit der intuitiven geometrischen Vorstellung definiert.

Ganz entsprechend geht man beim Aufbau der Mengenlehre vor. Es wird nicht definiert, was "Mengen" und "Elemente" sind, sondern es werden nur die Beziehungen definiert, die zwischen ihnen bestehen sollen und Konstruktionsprinzipien angegeben, um aus gegebenen Mengen weitere Mengen zu gewinnen. "Mengen" und "Elemente" werden also auf diese Weise nur implizit definiert, allerdings auch jetzt wieder in Übereinstimmung mit der intuitiven Vorstellung etwa im Sinne der Cantorschen "Definition".

1.2 Mengen und Elemente

Im Sinne der Ausführungen in der Einleitung betrachten wir gewisse nicht weiter definierte Objekte und zwar einerseits M e n g e n und andererseits E l e m e n t e .

Mengen werden meist durch große lateinische Buchstaben $A,B,C,\ldots,A_1,A_2,A_3,\ldots$, Elemente meist durch kleine lateinische Buchstaben $a,b,c,\ldots,a_1,a_2,a_3,\ldots$ angegeben.

Ferner benutzen wir die Symbole $\in$ und $\notin$ sowie zu einem Element x und einer Menge A die Zeichenreihen $x \in A$ und $x \notin A$.

Für Mengen, Elemente und die eingeführten Symbole wird nun axiomatisch die Gültigkeit gewisser Aussagen vorausgesetzt. Diese formulieren wir als Axiome.

(M 1) A x i o m d e r E l e m e n t e b e z i e h u n g u n d d e r E x i s t e n z

a) Für jedes Element x und jede Menge A besteht genau eine der beiden Beziehungen:
$x \in A$, in Worten "x ist Element von A" ,
$x \notin A$, in Worten "x ist nicht Element von A" .

b) Es gibt mindestens eine Menge.

c) Zu jedem Element x gibt es mindestens eine Menge A mit $x \in A$.

Für $x \in A$ werden außer der angegebenen Formulierung auch die Sprechweisen "x liegt in A" oder "x enthalten in A" oder "x in A" oder "x aus A" benutzt. Entsprechend werden für $x \notin A$ auch die Formulierungen "x liegt nicht in A" oder "x nicht enthalten in A" oder "x nicht in A" oder "x nicht aus A" verwendet.

Wir weisen darauf hin, daß man zum Aufbau der Mengenlehre die Forderung c) vermeiden kann, doch ist diese für unsere Zwecke bequem und entspricht auch völlig der intuitiven Vorstellung, daß es Elemente "nur als Elemente von Mengen" gibt. Ferner könnte man die Forderung der Existenz einer Menge in b) auf später verschieben oder ganz weglassen. Doch gehen wir ja von der Vorstellung aus, daß es Mengen geben soll, denn sonst würden wir keine Theorie darüber machen. Die Existenz einer Menge folgt auch nach c), wenn man die Existenz eines Elementes fordert. Umgekehrt folgt auf Grund von b) und weiteren Axiomen die Existenz von Elementen, insbesondere wird sich ergeben, daß jede Menge auch Element ist.

1.3 Gleichheit und Teilmengen

Dem Begriff der Menge liegt die Vorstellung zu Grunde, daß eine Menge allein durch ihre Elemente bestimmt ist. Um diese Vorstellung in einem Axiom zu erfassen, drücken wir sie zunächst wie folgt aus:"Haben zwei Mengen dieselben Elemente, so sind die Mengen gleich". Es gibt also nichts weiteres, worin sich diese beiden Mengen noch unterscheiden könnten. Wir verlangen daher für den Begriff der Menge, daß das folgende Axiom gilt.

(M 2) A x i o m d e r G l e i c h h e i t

$$\forall x\,[x \in A \Longleftrightarrow x \in B] \Rightarrow A = B\,.$$

Umgekehrt gilt wegen der Eigenschaften der Gleichheit (siehe I.1.3)

$$A = B \Rightarrow \forall x\,[x \in A \Longleftrightarrow x \in B]\,,$$

das heißt, sind zwei Mengen gleich, so haben sie dieselben Elemente. Gilt nämlich $A = B$ und $x \in A$, so gilt auch $x \in B$, da man A durch B ersetzen darf. Ebenso folgt aus $A = B$ und $x \in B$ auch $x \in A$.

Während durch ein Axiom gefordert wird, daß eine gewisse Aussage (im Rahmen der zu entwickelnden Theorie) als wahr zu betrachten ist, wird durch eine Definition eine Bezeichnung oder Symbolik für einen bestimmten Sachverhalt eingeführt. Dabei bleibt es zunächst offen, ob ein solcher Sachverhalt überhaupt existieren kann. Allerdings wird man nur dann eine Definition einführen, wenn man von der Existenz und Bedeutung des definierten Begriffes überzeugt ist. Wir sehen dies am Beispiel der folgenden Definition einer Teilmenge einer gegebenen Menge.

DEFINITION:

1) Die Menge A heißt T e i l m e n g e oder U n t e r m e n g e der Menge B, in Zeichen $A \subset B$, genau dann, wenn jedes Element von A auch Element von B ist.
   Mit Symbolen geschrieben:
   $A \subset B :\Longleftrightarrow \forall x\,[x \in A \Rightarrow x \in B]$
2) Ist A nicht Teilmenge von B, so wird $A \not\subset B$ geschrieben.

3) A heißt e c h t e T e i l m e n g e von B, in Zeichen
$A \subsetneq B :\Longleftrightarrow A \subset B \wedge A \neq B$.

Ist A Teilmenge von B, so nennt man B auch O b e r m e n g e von A. Das Zeichen $\subset$ wird auch I n k l u s i o n genannt. Man beachte den Unterschied zwischen $\in$ = "ist Element von" und $\subset$ = "ist Teilmenge von".

Berücksichtigt man unsere Ausführungen in I.2.4 zur Auswahl der Subjekte, so kann in der Definition von $A \subset B$ an Stelle von $\forall x \,[\, x \in A \Longrightarrow x \in B]$ auch $\forall x \in A \,[\, x \in B]$ geschrieben werden, also

$$A \subset B :\Longleftrightarrow \forall x \in A \,[\, x \in B] \quad .$$

Aus der vorstehenden Definition erhält man unmittelbar die

FOLGERUNG:
1) R e f l e x i v i t ä t : $A \subset A$
2) T r a n s i t i v i t ä t : $A \subset B \wedge B \subset C \Longrightarrow A \subset C$
3) A n t i s y m m e t r i e : $A \subset B \wedge B \subset A \Longrightarrow A = B$

Sind $a_1, a_2, \ldots, a_t$ die Elemente einer Menge A , dann benutzt man auch die Schreibweise $A = \{a_1, a_2, \ldots a_t\}$. Dabei wird nicht vorausgesetzt, daß die Elemente $a_1, a_2, \ldots, a_t$ alle voneinander verschieden sind. Zum Beispiel gilt

$$\{1 \,,\, 2\} = \{2 \,,\, 1 \,,\, 2 \,,\, 1 \,,\, 1\} \quad ,$$

denn jedes Element der links stehenden Menge ist in der rechts stehenden Menge enthalten und umgekehrt. Nach (M 2) besagt dies aber, daß diese Mengen gleich sind. Eine entsprechende Schreibweise $A = \{\ldots\}$ wird auch bei unendlichen Mengen verwendet, wenn es möglich ist, die Elemente von A eindeutig zu kennzeichnen. Davon werden wir alsbald Gebrauch machen, wenn wir uns mit der Frage beschäftigen, wie man aus einer Menge Teilmengen aussondern kann.

Später werden Mengen vorkommen, deren Elemente selbst wieder Mengen sind. Zum Beispiel wird sich ergeben, daß zu jeder Menge A die Menge $\{A\}$ existiert, das heißt die Menge, deren einziges Element A ist. Ist etwa $A = \{1 \,,\, 2\}$ eine

Menge, wie schon zuvor vorausgesetzt, dann gilt $A \neq \{A\}$, denn A besitzt die Elemente 1 und 2 , während $\{A\}$ das einzige Element A besitzt. Ausführlich geschrieben haben wir also $\{1 , 2\} \neq \{\{1 , 2\}\}$. Ferner beachte man, daß zwar $A \in \{A\}$, aber nicht $A \subset \{A\}$ gilt !

Es erhebt sich natürlich die Frage, ob es Teilmengen gibt. Trivialer Weise ist A Teilmenge von A, so daß man nach echten Teilmengen von A fragen wird. Ein Prinzip zur Bildung von Teilmengen wird durch das folgende Axiom gegeben.

(M 3) T e i l m e n g e n a x i o m

Sei B eine Menge und sei $\mathfrak{A}(x)$ ein Prädikat. Dann gibt es eine Teilmenge A von B , die genau die Elemente $b \in B$ enthält, für die $\mathfrak{A}(b)$ wahr ist. Für A wird

$$A = \{b \mid b \in B \wedge \mathfrak{A}(b)\}$$

geschrieben.

Machen wir uns die Bedeutung des Teilmengenaxioms an Beispielen klar. Dabei soll vorausgesetzt werden, daß die folgenden Mengen bereits gegeben sind, obwohl diese tatsächlich erst später (in Kapitel VII) eingeführt werden.

$\mathbb{N} = \{1,2,3,\ldots\}$ = Menge der natürlichen Zahlen,
$\mathbb{Z} = \{0,\pm1,\pm2,\pm3,\ldots\}$ = Menge der ganzen Zahlen,
$\mathbb{Q}$ = Menge der rationalen Zahlen,
$\mathbb{R}$ = Menge der reellen Zahlen .

B e i s p i e l e f ü r T e i l m e n g e n

1) $\{x \mid x \in \mathbb{N} \wedge x \text{ gerade}\}$ = Menge der geraden natürlichen Zahlen

2) $\{x \mid x \in \mathbb{N} \wedge x < 10\} = \{1,2,3,\ldots,9\}$

3) $\{x \mid x \in \mathbb{N} \wedge x \text{ ist Primzahl}\}$ = Menge der Primzahlen

4) $\{x \mid x \in \mathbb{R} \wedge 1 \leq x \leq 2\}$
Diese Menge bezeichnet man auch als das abgeschlossene Intervall $[1,2]$, während $\{x \mid x \in \mathbb{R} \wedge 1 < x < 2\}$ als das offene Intervall $(1,2)$ bezeichnet wird.

5) Sei B eine Menge und seien $b_1,\ldots,b_n$ Elemente von B, dann ist

$$\{b_1,\ldots,b_n\} = \{b \mid b \in B \wedge (b = b_1 \vee b = b_2 \vee \ldots \vee b = b_n)\}$$

eine Teilmenge von B.

6) Sei $b \in B$, dann gilt $\{b\} \subset B$. Dies ist ein Spezialfall von 5).

Nimmt man im Teilmengenaxiom für $\mathcal{A}(x)$ ein Prädikat, das für kein $b \in B$ eine wahre Aussage liefert, so erhält man eine Teilmenge von B, die kein Element enthält und die daher die l e e r e T e i l m e n g e von B, in Zeichen $\emptyset$, genannt wird. Als Prädikat, das nach (M 1) von keinem $b \in B$ erfüllt wird, kann $b \notin B$ gewählt werden.

DEFINITION:

$$\emptyset := \{b \mid b \in B \wedge b \notin B\}$$

Durch diese Definition haben wir die Menge $\emptyset$ zunächst als Teilmenge von B definiert. Sei A irgendeine weitere Menge, dann gilt für die Mengen

$$\{a \mid a \in A \wedge a \notin A\} \quad , \quad \{b \mid b \in B \wedge b \notin B\} \quad ,$$

die beide kein Element enthalten, nach (M 2) die Gleichheit. Folglich hängt die Menge $\emptyset$ nicht von der Wahl der Obermenge B ab, sondern ist Teilmenge von jeder beliebigen Menge.

Wir hatten in (M 1) gefordert, daß mindestens eine Menge A existiert. Wie eben festgestellt, existiert dann auch die Menge $\emptyset$. Da $A = \emptyset$ nicht ausgeschlossen ist, ist also bisher nur die Existenz der leeren Menge $\emptyset$ sichergestellt. Die Existenz weiterer Mengen wird sich später aus (M 5) ergeben.

Wichtige Teilmengen sind der Durchschnitt und die Komplementärmenge, die jetzt definiert werden sollen.

DEFINITION:
Seien A und B Mengen.

1) Der D u r c h s c h n i t t von A und B, in Zeichen $A \cap B$, ist die Teilmenge der Elemente aus A, die auch in B liegen:

$$A \cap B := \{a \mid a \in A \wedge a \in B\}$$

2) Die K o m p l e m e n t ä r m e n g e von B in A , in Zeichen $A \setminus B$, ist die Teilmenge der Elemente aus A , die nicht in B liegen:

$$A \setminus B := \{a \mid a \in A \wedge a \notin B\} \quad .$$

Der Leser mache sich zur Übung die folgenden einfachen Eigenschaften klar.

FOLGERUNG:

1) $A \cap B = B \cap A$
2) $(A \cap B) \cap C = A \cap (B \cap C)$
3) $A \cap B \subset A \wedge A \cap B \subset B$
4) Gilt für eine Menge C: $C \subset A \wedge C \subset B$, dann folgt $C \subset (A \cap B)$
5) $A \setminus B = A \setminus (A \cap B)$
6) $A \setminus (A \setminus B) = A \cap B$
7) $A \setminus \emptyset = A$, $A \setminus A = \emptyset$.

Den Durchschnitt von zwei Mengen kann man zunächst für endlich viele Mengen verallgemeinern:

$$A_1 \cap A_2 \cap \ldots \cap A_n := \{a \mid a \in A_1 \wedge a \in A_2 \wedge \ldots \wedge a \in A_n\} ,$$

denn auch diese Bildung fällt unter das Teilmengenaxiom. Will man den Durchschnitt von "mehr" als nur endlich vielen Mengen bilden, so steht die folgende Möglichkeit zur Verfügung.

DEFINITION:

Sei $\mathfrak{M}$ eine Menge, deren Elemente selbst Mengen sind und sei $\mathfrak{M} \neq \emptyset$. Ferner sei $A_0 \in \mathfrak{M}$, dann wird als D u r c h s c h n i t t von $\mathfrak{M}$, in Zeichen $\bigcap_{A \in \mathfrak{M}} A$ definiert:

$$\bigcap_{A \in \mathfrak{M}} A := \{a \mid a \in A_0 \wedge \forall A \in \mathfrak{M} [a \in A]\} \quad .$$

Offensichtlich hängt diese Definition nicht von der Wahl eines $A_0 \in \mathfrak{M}$ ab; wir haben diese Schreibweise nur gewählt, um zu betonen, daß diese Definition unter das Teilmengenaxiom fällt. Es genügt jedoch

$$A = \{a \mid \forall A \in \mathfrak{M} [a \in A]\}$$

zu schreiben. Diese Menge ist dadurch ausgezeichnet, daß sie

die "größte" Menge ist, die Teilmenge von jedem $A \in \mathfrak{M}$ ist. Das bedeutet: Diese Menge ist Teilmenge von jedem $A \in \mathfrak{M}$ und wenn B eine Menge ist, die Teilmenge von jedem $A \in \mathfrak{M}$ ist, dann gilt

$$B \subset \bigcap_{A \in \mathfrak{M}} A \quad .$$

1.4 Vereinigungsmengen

Die zur Durchschnittsmenge "duale" Bildung ist die der Vereinigungsmenge. Daß diese existiert, fordert das nächste Axiom.

(M 4) V e r e i n i g u n g s m e n g e n a x i o m

1) Sind A und B zwei Mengen, dann gibt es eine Menge, V e r e i n i g u n g s m e n g e von A und B genannt und mit $A \cup B$ bezeichnet, die genau die Elemente enthält, die in A oder B enthalten sind:

$$A \cup B = \{ x \mid x \in A \vee x \in B \}$$

2) Sei $\mathfrak{M}$ eine Menge, deren Elemente selbst Mengen sind, dann gibt es eine Menge, V e r e i n i g u n g s m e n g e von $\mathfrak{M}$ genannt und mit $\bigcup_{A \in \mathfrak{M}} A$ bezeichnet, die genau die Elemente enthält, die in mindestens einem $A \in \mathfrak{M}$ liegen:

$$\bigcup_{A \in \mathfrak{M}} A = \{ x \mid \exists A \in \mathfrak{M} \; [x \in A] \}$$

Wir bemerken dazu zunächst, daß wir unter 1) die Vereinigungsmenge $A \cup B$ gefordert haben, da diese einerseits vernünftigerweise existieren sollte, andererseits nicht sichergestellt ist, daß man sie aus 2) erhält. Dazu müßte es eine Menge $\mathfrak{M}$ geben, die genau die Elemente A und B besitzt. Fordert man axiomatisch eine solche Menge $\mathfrak{M} = \{A, B\}$, dann kann man sich auf 2) beschränken. Umgekehrt ergibt sich aus 1) zusammen mit dem später folgenden Potenzmengenaxiom, daß die Menge $\{A, B\}$ existiert. Durch Induktion über n ergibt sich auch, daß zu endlich vielen Mengen $A_1, \ldots, A_n$ ebenfalls die Vereinigungsmenge existiert:

$$A_1 \cup \ldots \cup A_n = \{ x \mid x \in A_1 \vee \ldots \vee x \in A_n \} \; .$$

Während zur Definition von $\bigcap_{A\in\mathfrak{M}} A$ die Voraussetzung $\mathfrak{M} \neq \emptyset$ gemacht werden mußte (um das Teilmengenaxiom anwenden zu können), ist bei der Definition von $\bigcup_{A\in\mathfrak{M}} A$ auch $\mathfrak{M} = \emptyset$ zugelassen. Das Axiom (M 4) liefer jetzt

$$\bigcup_{A\in\emptyset} A = \emptyset ,$$

denn

$$\bigcup_{A\in\emptyset} A = \{x \mid \exists A \in \emptyset\, [x \in A]\} = \emptyset ,$$

da es kein $A \in \emptyset$ gibt, also auch kein Element eines A in $\bigcup_{A\in\emptyset} A$ enthalten sein kann.

Es folgen einige Rechenregeln, deren Beweise dem Leser zur Übung überlassen bleiben.

RECHENREGELN:

1) $A \cup B = B \cup A$
2) $(A \cup B) \cup C = A \cup (B \cup C)$
3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
4) Die de Morganschen Gesetze:
   $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$,
   $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

1.5 Potenzmengen

Zum Aufbau der Mengenlehre wird ein weiteres Axiom gebraucht, das einerseits sicherstellt, daß jede Menge auch Element einer Menge ist und andererseits zu einer gegebenen Menge die Konstruktion einer Menge mit einer größeren Elementezahl ermöglicht.

(M 5) Potenzmengenaxiom

Zu jeder Menge A gibt es eine Menge, Potenzmenge von A genannt und mit P(A) bezeichnet, die genau alle Teilmengen von A als Elemente enthält. Diese wird auch durch

$$P(a) = \{ U \mid U \subset A \}$$

bezeichnet.

Zur Übung betrachten wir einige Beispiele. So ist

$P(\emptyset) = \{\emptyset\}$ eine Menge mit einem Element ,

$P(\{a\}) = \{\emptyset, \{a\}\}$ eine Menge mit zwei Elementen ,

$P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ eine Menge mit vier Elementen, (falls $a \neq b$).

Allgemein gilt die

BEHAUPTUNG:
Ist A eine Menge mit n Elementen, dann ist P(A) eine Menge mit 2^n Elementen.

Beweis: Vollständige Induktion nach der Zahl n der Elemente.
Induktionsbeginn: $n = 0$, das heißt $A = \emptyset$. Dann ist $P(\emptyset) = \{\emptyset\}$ eine Menge mit $1 = 2^0$ Elementen.
Induktionsannahme: Die Behauptung sei richtig für alle Mengen mit höchstens n Elementen.
Induktionsschluß: Sei $A = \{a_1, \ldots, a_n, a_{n+1}\}$ eine Menge mit n+1 Elementen. Wir unterscheiden für die Teilmengen zwei Fälle.
1.Fall: Sei $U \subset A \wedge a_{n+1} \notin U$.
Dann ist $U \subset A_n := \{a_1, \ldots, a_n\}$. Die Menge A_n besitzt nach Induktionsannahme 2^n Teilmengen und jede ihrer Teilmengen ist auch Teilmenge von A . Also gibt es 2^n Teilmengen $U \subset A$ mit $a_{n+1} \notin U$.
2.Fall: Sei $V \subset A \wedge a_{n+1} \in V$.
Wir überlegen, daß man alle solchen Teilmengen V in der Form $V = U \cup \{a_{n+1}\}$ aus genau allen Teilmengen $U \subset A_n$ erhält.
Zunächst ist klar, daß aus $U \subset A_n$ folgt:

$$V := U \cup \{a_{n+1}\} \subset A \wedge a_{n+1} \in V \quad .$$

Gilt $U_1 \subset A_n \wedge U_2 \subset A_n \wedge U_1 \neq U_2$, dann folgt auch

$$U_1 \cup \{a_{n+1}\} \neq U_2 \cup \{a_{n+1}\} \quad .$$

Sei umgekehrt $V \subset A \wedge a_{n+1} \in V$, dann folgt

$$V \setminus \{a_{n+1}\} \subset A_n \wedge (V \setminus \{a_{n+1}\}) \cup \{a_{n+1}\} = V \ ,$$

also erhält man genau alle solchen V in der Form $V = U \cup \{a_{n+1}\}$ mit $U \subset A_n$. Da nach Induktionsannahme genau 2^n $U \subset A_n$ existieren, müssen folglich genau 2^n $V \subset A$ mit $a_{n+1} \in V$ existieren.

Da jede Teilmenge von A genau unter einem der beiden Fälle vorkommt, gibt es $2^n + 2^n = 2^{n+1}$ Teilmengen von A .//

Bei unserem Aufbau war durch (M 1) - (M 4) nur die Existenz der leeren Menge gesichert. (M 5) liefert weitere Mengen wie $P(\emptyset)$, $P(P(\emptyset)) = P(\{\emptyset\})$, $P(P(P(\emptyset))) = P(\{\emptyset , \{\emptyset\}\})$, $P(P(P(P(\emptyset)))) = P(\{\emptyset , \{\emptyset\} , \{\{\emptyset\}\} , \{\emptyset , \{\emptyset\}\}\})$, ... mit $1 , 2 , 2^2 , 2^4 , \ldots$ Elementen, und nach (M 4) existieren auch deren Teilmengen. Damit erhält man insbesondere zu jeder natürlichen Zahl n eine Menge mit 2^n Elementen. Will man die Existenz von unendlichen Mengen, die man zum Beispiel braucht, um die Menge $\mathbb{N}$ der natürlichen Zahlen einführen zu können, dann bedarf es eines weiteren Axioms. Darauf kommen wir im VII. Kapitel zurück.

Da $A \in P(A)$ für jede Menge A gilt, ist jede Menge auch Element. Darüber hinaus gilt folgendes: Sind $A_1,\ldots,A_n$ Mengen, dann gibt es eine Menge $\{A_1,\ldots,A_n\}$, die genau die Mengen $A_1,\ldots,A_n$ als Elemente enthält. Wie man sich leicht klar macht, gilt nämlich, wenn noch

$$M := (\ldots((A_1 \cup A_2) \cup A_3)\ldots) \cup A_n$$

gesetzt wird:

$$\{A_1,\ldots,A_n\} = \{X \mid X \in P(M) \wedge (X=A_1 \vee X=A_2 \vee \ldots \vee X=A_n)\} .$$

Für die Potenzmengenbildung gelten folgende Rechenregeln, deren Beweise dem Leser zur Übung überlassen bleiben.

RECHENREGELN:

1) $P(A) \cap P(B) = P(A \cap B)$
2) $P(A) \cup P(B) \subset P(A \cup B)$
3) $A \subset B \Rightarrow P(A) \subset P(B)$
4) $\bigcap_{U \in P(A)} U = \emptyset$, $\bigcup_{U \in P(A)} U = A$.

1.6 Ausblick , Kardinal- und Ordinalzahlen

Wir wollen zum Schluß dieser Einführung in die Mengenlehre auf drei Gesichtspunkte hinweisen, die für den weiteren

Aufbau der Mengenlehre von Bedeutung sind. Sie sollen einen Eindruck davon geben, welche Rolle die Mengenlehre als eigenständige mathematische Theorie spielt. Dabei werden wir auf Beweise verzichten; diese findet der interessierte Leser in Büchern über Mengenlehre.

1) EINORDNUNG DES ZAHLBEGRIFFES

Bisher wurde - wenn auch in vermeidbarer Weise - vom Begriff der natürlichen Zahl Gebrauch gemacht, und die Zahlenmengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ wurden für Beispiele benutzt. Bei einem axiomatischen Aufbau der Mengenlehre kann man jedoch insbesondere die Menge $\mathbb{N}$ aufgrund von entsprechenden Axiomen im Rahmen der Mengenlehre gewinnen und ferner zeigen, daß $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und die Menge $\mathbb{C}$ der komplexen Zahlen tatsächlich Mengen im Sinne dieser Mengenlehre sind. Da ein solcher systematischer, axiomatischer Aufbau sowohl in der Zielsetzung als auch im Umfang über den Rahmen dieser Darstellung hinausgehen würde, entwickeln wir zwar die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ im VII. Kapitel, jedoch ohne dabei einen solchen axiomatischen Aufbau streng einzuhalten.

2) ANTINOMIEN DER MENGENLEHRE, DER KLASSENBEGRIFF

In der historischen Entwicklung der Mengenlehre hat man sich zunächst bei der Bildung von Mengen keine Beschränkung auferlegt. Man glaubte, daß durch jede "Bedingung" (Prädikat) die "Erfüllungsmenge dieser Bedingung", das heißt die Menge aller Objekte , die dieser Bedingung genügen, definiert würde. Danach wäre es also sinnvoll, von der "Menge aller Mengen" zu sprechen. B. R u s s e l l (1872 - 1970) bemerkte als erster, daß dieses Verfahren zu Widersprüchen (Russellsche Antinomie) führt.

Wir wollen überlegen, daß zu jeder Menge A eine Menge B mit $B \notin A$ existiert, so daß es keine Menge geben kann, die jede Menge als Element enthält. Nach dem Axiom (M 3) gibt es zu jeder Menge A die Teilmenge

$$U := \{ a \mid a \in A \wedge a \text{ ist Menge} \wedge a \notin a \} \quad ;$$

da jede Menge auch Element ist ($A \in \{A\}$), hat die Aussage $a \notin a$ einen Sinn.
Behauptung: $U \notin A$.
Beweis: Angenommen $U \in A$, dann unterscheiden wir zwei Fälle.
1. Fall: $U \notin U$, dann folgt (da $U \in A$) $U \in U$. Widerspruch !
2. Fall: $U \in U$, dann folgt (da $U \in A$) $U \notin U$. Widerspruch !
Also führt die Annahme $U \in A$ in jedem Falle zum Widerspruch, das heißt, es muß $U \notin A$ gelten.

Wir sind der hier aufgezeigten Gefahr - etwa die "Menge aller Mengen" bilden zu wollen - dadurch entgangen, daß im Axiom (M 3) die "Erfüllungsmenge" zu einem Prädikat $\mathfrak{A}(x)$ auf die Elemente einer bereits vorhandenen Menge beschränkt wurde.

Auf der anderen Seite besteht aber der Wunsch, so etwas wie die "Zusammenfassung" aller Mengen oder aller Gruppen oder aller topologischen Räume usw. mathematisch in den Griff zu bekommen. Dies ist in der Tat möglich und hat zu einer Theorie der Klassen geführt. Es gibt dann im Sinne dieser Theorie die Klasse aller Mengen, die Klasse aller Gruppen usw. Die Axiome für die Klassen müssen notwendig von den Axiomen für die Mengen abweichen, da sonst "Klasse" nur ein anderer Ausdruck für "Menge" wäre. Kurz kann man sagen, daß man mit Klassen "nicht so viel machen darf" wie mit Mengen. In einer solchen Theorie der Klassen werden dann die Mengen als diejenigen Klassen ausgesondert, die (mindestens) in einer Klasse als Element enthalten sind.

3) KARDINALZAHLEN UND ORDINALZAHLEN

Das Hauptziel der Mengenlehre als selbstständiger mathematischer Theorie besteht darin, unendliche Mengen zu untersuchen und zu klassifizieren. Dies kann unter dem Gesichtspunkt gesehen werden, den Begriff der natürlichen Zahl einerseits als Anzahl (= Kardinalzahl) und andererseits versehen mit der Anordnung der natürlichen Zahlen (= Ordinalzahl) auf beliebige unendliche Mengen auszudehnen.

Die Untersuchung der Kardinalzahlen und der Ordinalzahlen, insbesonere ihrer Arithmetik und weiterer damit zusammenhängender Fragen ist der Hauptgegenstand der Mengenlehre. Um dies für den Leser anzudeuten, geben wir hier zwei verschiedene Wege zur Einführung der Kardinal- und Ordinalzahlen an. Dabei muß allerdings von Begriffen Gebrauch gemacht werden, die in diesem Buch erst später vorkommen (siehe jeweils die Hinweise).

1. Weg

Zwei Mengen A und B heißen ä q u i v a l e n t oder g l e i c h m ä c h t i g , in Zeichen $A \sim B$, wenn eine Bijektion (= umkehrbar eindeutige Abbildung, siehe III.1.6) von A nach B existiert. Es gilt dann für beliebige Mengen A,B,C :

Reflexivität : $A \sim A$
Symmetrie : $A \sim B \Rightarrow B \sim A$
Transitivität : $A \sim B \wedge B \sim C \Rightarrow A \sim C$.

Die K a r d i n a l z a h l von A , in Zeichen $|A|$, ist dann die Klasse aller zu A äquivalenten Mengen. Die Problematik dieser Definition liegt darin, daß die Klasse $|A|$ keine Menge ist.

Gilt $B \in |A|$, das heißt $B \sim A$, dann heißt B ein Repräsentant von $|A|$. Dafür gilt $B \in |A| \Longleftrightarrow |B| = |A|$. Für zwei Kardinalzahlen kann nun eine Anordnungsbeziehung im Sinne von "größer" und "kleiner" erklärt werden. Man definiert: Die Kardinalzahl $|A|$ heißt kleiner als $|B|$, in Zeichen $|A| \leq |B|$, wenn A zu einer Teilmenge von B äquivalent ist, und $|A|$ heißt echt kleiner als $|B|$, in Zeichen $|A| < |B|$, wenn $|A| \leq |B| \wedge |A| \neq |B|$ gilt. Man macht sich leicht klar, daß diese Definition nicht von der Wahl der Repräsentanten A und B abhängt.

Entscheidend dafür, daß sich die Beziehung $\leq$ so verhält, wie man das auf Grund der Schreibweise und vom Falle endlicher Mengen her erwartet, ist der Satz von C a n t o r - B e r n s t e i n :

Ist A zu einer Teilmenge von B äquivalent und ist B zu einer Teilmenge von A äquivalent, dann sind A und B äquivalent, das heißt, es gilt

$$|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B| \ .$$

Damit kann gezeigt werden, daß für zwei beliebige Kardinalzahlen $|A|$ und $|B|$ stets genau eine der drei folgenden Bedingungen erfüllt ist:

$$|A| < |B| \ , \quad |A| = |B| \ , \quad |B| < |A| \ .$$

Es folgt dann für beliebige Mengen A,B,C :

Reflexivität: $|A| \leq |A|$

Transitivität: $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$

Antisymmetrie: $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |B|$

Ist P(A) die Potenzmenge von A , dann gilt für jede Menge A

$$|A| < |P(A)| \ ,$$

so daß also im Sinne von $\leq$ keine größte Kardinalzahl existieren kann.

Berühmt ist das von G. C a n t o r 1884 aufgeworfene Kontinuumsproblem. Es handelt sich um die Frage, ob es eine Menge M gibt, deren Mächtigkeit zwischen der von $\mathbb{N}$ und $\mathbb{R}$ liegt, das heißt, für die gilt

$$|\mathbb{N}| < |M| < |\mathbb{R}| \ .$$

Cantor vermutete, daß keine solche Menge existiere und diese Vermutung wurde dann die Kontinuumshypothese genannt. Von D. H i l b e r t wurde die Bedeutung dieses Problems unterstrichen (1900). Auf Grund von Arbeiten von K. G ö d e l (1938) und P.J. C o h e n (1963) weiß man heute, daß das Kontinuumsproblem "unentscheidbar" ist. Gödel zeigte zunächst, daß folgendes gilt: Nimmt man zu einem Axiomensystem der Mengenlehre als Axiom hinzu, daß die Kontinuumshypothese gilt, so ist dies vergrößerte Axiomensystem widerspruchsfrei. Ein Axiomensystem heißt dabei widerspruchsfrei, wenn sich auf Grund des Axiomensystems nicht zugleich eine Aussage und ihre Negation beweisen lasse. Nach dem Ergebnis von Gödel folgt, daß auf der Grundlage des Axiomensystems der Mengenlehre die Negation der Kontinuumshypothese nicht beweisbar

ist, denn sonst wäre das vergrößerte Axiomensystem doch widerspruchsvoll. Cohen schließlich lieferte die Aussage, daß man auch ein widerspruchsfreies Axiomensystem erhält, wenn man zu den Axiomen der Mengenlehre als Axiom hinzunimmt, daß die Kontinuumshypothese nicht gilt. Also ist auf der Grundlage des Axiomensystems der Mengenlehre auch die Richtigkeit der Kontinuumshypothese nicht beweisbar. Beide Ergebnisse zusammen liefern die Aussage, daß das Kontinuumsproblem "unentscheidbar" ist (jedenfalls auf der Grundlage des üblichen Axiomensystems der Mengenlehre).

Identifiziert man die natürlichen Zahlen mit den endlichen Kardinalzahlen, so kann man deren Addition und Multiplikation auf beliebige Kardinalzahlen verallgemeinern. Zu den Kardinalzahlen $|A|$ und $|B|$ gibt es stets $A_1 \in |A|$, $B_1 \in |B|$ mit $A_1 \cap B_1 = \emptyset$. Dann wird als S u m m e definiert:

$$|A| + |B| := |A_1 \cup B_1| \ .$$

Ist $A \times B$ die Produktmenge von A und B (siehe den folgenden §3), dann wird als P r o d u k t definiert:

$$|A| \cdot |B| := |A \times B| \ .$$

Diese Definitionen sind von der Wahl der Repräsentanten unabhängig. Sie können auch sofort auf Summen und Produkte der Form

$$\sum_{i \in I} |A_i| \quad , \qquad \prod_{i \in I} |A_i|$$

ausgedehnt werden, wenn nur I eine Menge ist. Dies soll für die Summe ausgeführt werden. Zu jedem $i \in I$ kann in $|A_i|$ ein Repräsentant C_i so gewählt werden, daß $C_i \cap C_j = \emptyset$ für alle $i,j \in I$ mit $i \neq j$ gilt. Man wähle zum Beispiel $C_i = A_i \times \{i\} = \{(a,i) \mid a \in A_i\}$. Da I eine Menge ist, ist $\bigcup_{i \in I} C_i$ eine Menge, und man setze nun

$$\sum_{i \in I} |A_i| := \Big| \bigcup_{i \in I} C_i \Big| \ .$$

Sind A und I zwei Kardinalzahlen, so kann auch $|A|^{|I|}$ definiert werden:

$$|A|^{|I|} := \prod_{i \in I} |A_i| \quad \text{mit} \quad A_i = A \text{ für jedes } i \in I \ .$$

Wir wollen nun einige Beispiele für das Rechnen mit Kardinalzahlen angeben. Dazu seien $0,1,2,\ldots$ die Kardinalzahlen der Mengen mit null, eins, zwei, ... Elementen; ferner bezeichne

$$\aleph_0 = |\mathbb{N}| \quad , \qquad \mathfrak{c} = |\mathbb{R}| \ .$$

Dann gilt:

$$\begin{aligned}
&\aleph_0 + n = \aleph_0 \cdot n = \aleph_0 \quad \text{für jedes } n \in \mathbb{N} \ , \\
&\aleph_0 + \aleph_0 = \aleph_0 \quad , \quad \aleph_0 \cdot \aleph_0 = \aleph_0 \ , \\
&\aleph_0 + \mathfrak{c} = \mathfrak{c} + \mathfrak{c} = \aleph_0 \cdot \mathfrak{c} = \mathfrak{c}\,\mathfrak{c} = \mathfrak{c} \ , \\
&\aleph_0^{\,n} = \aleph_0 \quad , \quad \mathfrak{c}^{\,n} = \mathfrak{c} \quad \text{für jedes } n \in \mathbb{N} \ , \\
&2^{\aleph_0} = n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{c}^{\aleph_0} = \mathfrak{c} \quad \text{für jedes } n \in \mathbb{N} \ , \\
&2^{\mathfrak{m}} > \mathfrak{m} \quad \text{für jede Kardinalzahl } \mathfrak{m} \ .
\end{aligned}$$

Zur letzten Formel beachte man: Ist $\mathfrak{m} = |M|$, dann folgt $|P(M)| = 2^{\mathfrak{m}}$.

Wir kommen jetzt zur Definition der Ordinalzahlen. Seien A und B zwei geordnete Mengen mit den Ordnungen $\leqq_1$ und $\leqq_2$ (siehe dazu III.3). Diese geordneten Mengen heißen ä h n l i c h , in Zeichen $A \simeq B$, wenn eine Bijektion (siehe III.1) $\sigma : A \longrightarrow B$ so existiert, daß gilt

$$\forall a_1, a_2 \in A \left[a_1 \leqq_1 a_2 \Longleftrightarrow \sigma(a_1) \leqq_2 \sigma(a_2) \right] \ ,$$

das heißt, σ ist eine mit den Ordnungen verträgliche Bijektion.

Man beachte bei dieser und allen weiteren Überlegungen, daß eine Menge mehrere Ordnungen besitzen kann (und auch besitzt, wenn sie mehr als ein Element enthält). Die Beziehung $A \simeq B$ hängt also sowohl von den Mengen A und B, als auch von ihren Ordnungen ab. Die Klasse aller zu der geordneten Menge A ähnlichen geordneten Mengen wird mit $\langle A \rangle$ bezeichnet und O r d n u n g s t y p von A genannt.

Ist die Ordnung von A sogar eine Wohlordnung (siehe III.3), dann heißt $\langle A \rangle$ O r d i n a l z a h l von A. Der Ordnungstyp ist also der allgemeinere Begriff, während sich der Begriff Ordinalzahl nur auf wohlgeordnete Mengen bezieht.

Um zwischen zwei Ordinalzahlen eine Anordnung definieren zu können, braucht man den Begriff des Abschnitts. Sei A eine

wohlgeordnete Menge mit der Ornung $\leq$, wofür wir auch $(A,\leq)$ schreiben. Eine Teilmenge B von A heißt A b s c h n i t t von A : $\Longleftrightarrow$

$$\forall x,y \in A \,[\, x \in B \wedge y \leq x \Rightarrow y \in B \,] \ .$$

Es ist dann klar, daß ein Abschnitt B von $(A,\leq)$ mit der Ordnung $\leq$ von A selbst wieder eine wohlgeordnete Menge ist. Man definiert nun für zwei Ordinalzahlen $\langle A\rangle$ und $\langle B\rangle$:

$$\langle B\rangle \leq \langle A\rangle \ : \Longleftrightarrow \text{ B ist zu einem Abschnitt von A ähnlich.}$$

Es gelten dann die gleichen Eigenschaften wie für die Anordnung zwischen Kardinalzahlen.

Um die A d d i t i o n zwischen zwei Ordinalzahlen $\langle A\rangle$ und $\langle B\rangle$, wobei $\leqq_1$ die Ordnung von A und $\leqq_2$ die Ordnung von B seien , zu definieren, kann $A \cap B = \emptyset$ angenommen werden. Dann sei

$$\langle A\rangle + \langle B\rangle := \prec A \cup B \succ$$

mit der folgenden Anordnung: Für $x,y \in A \cup B$ gelte

$$x \leq y \ : \Longleftrightarrow \begin{cases} \text{falls } x,y \in A \text{ und } x \leqq_1 y \text{ gilt} \\ \text{falls } x,y \in B \text{ und } x \leqq_2 y \text{ gilt} \\ \text{falls } x \in A \text{ und } y \in B \text{ gilt .} \end{cases}$$

Man beachte, daß die so definierte Addition nicht kommutativ ist.

Schließlich definiert man als Produkt

$$\langle A\rangle \cdot \langle B\rangle := \langle A \times B\rangle$$

mit der folgenden Ordnung von $A \times B$: Es sei für $a_1,a_2 \in A$, $b_1,b_2 \in B$

$$(a_1,b_1) \leq (a_2,b_2) \ : \Longleftrightarrow \begin{cases} \text{falls } a_1 \neq a_2 \wedge a_1 \leqq_1 a_2 \\ \text{falls } a_1 = a_2 \wedge b_1 \leqq_2 b_2 \end{cases} .$$

Mit diesen Andeutungen wollen wir uns begnügen. Für das Rechnen mit Ordinalzahlen sei auf die Literatur verwiesen.

Worin liegt nun die Problematik dieser Einführung der Kardinal- und Ordinalzahlen, auf die wir anfangs schon hingewiesen haben ? Bei vielen Überlegungen ist es wünschenswert,

Mengen von Kardinalzahlen oder Mengen von Ordinalzahlen zu betrachten. Dies ist jedoch, da Kardinalzahlen und Ordinalzahlen Klassen aber keine Mengen sind, verboten. Was ist da zu tun ? Wie die Literatur über Mengenlehre zeigt, kann man sich in verschiedener, mehr oder weniger fragwürdiger Weise aus der Affaire ziehen.

Dazu schreibt G. C a n t o r (1895):
""Mächtigkeit" oder "Cardinalzahl" von M nennen wir den Allgemeinbegriff, welcher mit Hülfe unseres activen Denkvermögens dadurch aus der Menge M hervorgeht, dass von der Beschaffenheit ihrer verschiedenen Elemente m und von der Ordnung ihres Gegebenseins abstrahiert wird."

F. H a u s d o r f f gibt folgende Erklärung (1914):
"Mengen eines Systems, die einer gegebenen Menge und damit auch untereinander äquivalent sind, haben etwas Gemeinsames, das im Falle endlicher Mengen die Anzahl der Elemente ist und das man auch im allgemeinen Falle die Anzahl oder Kardinalzahl oder Mächtigkeit nennt. Über die absolute Beschaffenheit dieses neu eingeführten Etwas kann man allerhand verschiedene Auffassungen hegen.... Wir werden uns einfach auf den formalen Standpunkt stellen und sagen: einem System von Mengen A ordnen wir eindeutig ein System von Dingen $\mathfrak{a}$ zu derart, daß äquivalenten Mengen und nur solchen dasselbe Ding entspricht.... Dieses neue Ding oder Zeichen nennen wir Kardinalzahl oder Mächtigkeit ...".

E. K a m k e nimmt folgenden Standpunkt ein (1962):
"Unter einer Kardinalzahl oder Mächtigkeit $\mathfrak{m}$ wird ein beliebiger Repräsentant M aus einer Klasse von untereinander äquivalenten Mengen verstanden".

Andere Autoren schränken die zur Konkurrenz zugelassenen Mengen so ein, daß die Klasse aller äquivalenten Mengen wieder eine Menge ist.

Die heute übliche Möglichkeit der Einführung von Kardinal- und Ordinalzahlen, die wohldefinierte Begriffe liefert und

mengentheoretische Schwierigkeiten vermeidet, wird nachstehend angegeben.(Siehe zum Beispiel Paul R. Halmos:"Naive set theory", D.van Nostrand Comp.,1960).

2. Weg

Hierbei werden zunächst Ordinalzahlen als gewisse, eindeutig bestimmte wohlgeordnete Mengen definiert und sodann Kardinalzahlen als gewisse Ordinalzahlen. An Stelle der Klassen ähnlicher wohlgeordneter Mengen bzw. der Klassen äquivalenter Mengen treten hier von vornherein bestimmte Repräsentanten dieser Klassen.

Sei $(A,\leq)$ eine wohlgeordnete Menge. Zu $a \in A$ definiert man

$$Ab(a) := \{ x \mid x \in A \wedge x < a \}$$

als Abschnitt von a .

Definiert man die Zahlen aus $\mathbb{N}_0$ in folgender Weise :

$$0 := \emptyset$$
$$1 := \{0\}$$
$$2 := \{0,1\}$$

und induktiv

$$n := \{0,1,\ldots n-1\} \quad ,$$

dann folgt für jedes $n \in \mathbb{N}_0$

$$Ab(n) = \{ 0,1,\ldots,n-1\} = n \quad ,$$

wobei die natürliche Ordnung von $\mathbb{N}_0$ zugrunde gelegt wurde.

Die entsprechende Eigenschaft wird nun benutzt, um in der Klasse aller untereinander ähnlichen wohlgeordneten Mengen einen Repräsentanten auszuzeichnen, der dann Ordinalzahl genannt wird.

DEFINITION:
Eine wohlgeordnete Menge $(A,\leq)$ heißt O r d i n a l z a h l :
$\Longleftrightarrow \forall a \in A \, [\, Ab(a) = a]$.

Entscheidend für die Zweckmäßigkeit dieser Definition ist die Tatsache, daß jede wohlgeordnete Menge zu genau einer Ordinalzahl ähnlich ist. Mit anderen Worten: In jeder Klasse ähnlicher wohlgeordneter Mengen liegt genau eine solche

Ordinalzahl. Ist $(M,\overset{\prec}{=})$ eine wohlgeordnete Menge und ist $(A,\leq)$ die dazu ähnliche Ordinalzahl, dann wird A oder genauer $(A,\leq)$ die Ordinalzahl von $(M,\overset{\prec}{=})$ genannt , in Zeichen

$$\mathrm{Ord}(M) = \mathrm{Ord}(M,\overset{\prec}{=}) := A = (A,\leq) \quad .$$

Sind $(A_1,\leqq_1)$ und $(A_2,\leqq_2)$ Ordinalzahlen, dann gilt stets, daß die erste Abschnitt von der zweiten oder umgekehrt ist, sodaß $A_1 \subset A_2$ oder $A_2 \subset A_1$ gilt. Darüber hinaus gilt, daß jede Menge von Ordinalzahlen bezüglich der Inklusion als Ordnung wohlgeordnet ist.

Sei nun M eine beliebige Menge, dann ist die Klasse aller Ordinalzahlen $(A,\leq)$ mit $M \sim A$ sogar eine Menge und diese besitzt ein kleinstes Element $(A_0,\leqq_0)$. Diese Ordinalzahl $(A_0,\leqq_0)$ wird nun als Kardinalzahl von M definiert:

$$\mathrm{Kard}(M) := (A_0,\leqq_0)$$

Danach sind also die Kardinalzahlen gewisse "kleinste" Ordinalzahlen. Genauer: Die in der Menge aller gleichmächtigen Ordinalzahlen enthaltene kleinste Ordinalzahl heißt Kardinalzahl. Damit hat man Definitionen für Ordinal- und Kardinalzahlen, bei denen mengentheoretische Schwierigkeiten vermieden werden.

§ 2 Paare und Produktmengen

2.1 Paare

Seien a und b zwei Elemente. Wegen (M 1) gibt es dann eine Menge M mit $a \in M$ und eine Menge N mit $b \in N$. Folglich existieren die Mengen

$$\{a\} = \{m \mid m \in M \wedge m = a\} \quad ,$$
$$\{a,b\} = \{x \mid x \in M \cup N \wedge (x = a \vee x = b)\} \quad .$$

Da $\{a\}$ und $\{a,b\}$ Mengen sind, existiert ferner die Menge $\{\{a\}, \{a,b\}\}$ (wie in 1.5 gezeigt).

DEFINITION:
Das P a a r (a,b) der Elemente a und b ist die Menge, deren Elemente die Mengen $\{a\}$ und $\{a,b\}$ sind:

$$(a,b) := \{\{a\}, \{a,b\}\} \quad ;$$

a heißt das erste Element des Paares (a,b),
b heißt das zweite Element des Paares (a,b).

Statt der Bezeichnung "Paar" wird in der Literatur auch oft "geordnetes Paar" verwendet. Ebenso gibt es beide Bezeichnungen bei Tripeln, n-Tupeln usw.

Es mag zunächst überraschend erscheinen, daß man den so anschaulich erscheinenden Begriff des Paares auf eine nicht ganz naheliegende mengentheoretische Definition stützt. Bei dieser Gelegenheit kann man die Frage stellen, welche Rolle die Anschauung in der Mathematik spielt. Die Bedeutung der Anschauung liegt darin, daß sie uns zu Ideen, Begriffen, Sachverhalten und Beweisansätzen anregt, die dann jedoch unabhängig von der Anschauung mathematisch präzisiert werden müssen.

Die mathematische Präzisierung des Begriffes "Paar" besteht in der vorstehenden mengentheoretischen Definition, die ihre Rechtfertigung durch die folgende Behauptung erhält.

BEHAUPTUNG:
Für die Paare (a,b) und (x,y) gilt:

$$(a,b) = (x,y) \iff a = x \wedge b = y \quad .$$

Beweis: "$\Leftarrow$": Nach den Eigenschaften der Gleichheit (siehe 1.3) darf man im Paar (a,b) a durch x und b durch y ersetzen.
"$\Rightarrow$": Wir unterscheiden zwei Fälle.
1.Fall: a = b . Dann folgt $(a,b) = (a,a) = \{\{a\}, \{a,a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$. Wegen $(x,y) = \{\{x\}, \{x,y\}\} = (a,b) = \{\{a\}\}$ folgt $\{x\} = \{a\}$ und $\{x,y\} = \{a\}$, also x = a und y = a = b.
2.Fall: $a \neq b$. Dann folgt, daß $\{a,b\}$ zwei Elemente hat und daher gilt $\{a,b\} = \{x,y\}$, also auch $x \neq y$. Dann ergibt sich $\{x\} = \{a\}$, also x = a und wegen $\{a,b\} = \{x,y\}$ folgt schließlich y = b .//

Die Behauptung entspricht der anschaulichen Vorstellung, daß zwei Paare genau dann gleich sind, wenn sowohl die ersten als auch die zweiten Komponenten gleich sind.

2.2 Produktmengen

Seien jetzt zwei Mengen A und B gegeben und seien $a \in A$, $b \in B$. Dann ist $(a,b) = \{\{a\},\{a,b\}\}$ offenbar ein Element der Menge $P(P(A \cup B))$, denn $\{a\} \in P(A \cup B)$, $\{a,b\} \in P(A \cup B)$ und folglich $(a,b) \in P(P(A \cup B))$.

DEFINITION:
Seien A und B Mengen.

$$A \times B := \{x \mid x \in P(P(A \cup B)) \wedge \exists a \in A,\ b \in B [x = (a,b)]\}$$
$$= \{(a,b) \mid a \in A \wedge b \in B\}$$

heißt das P r o d u k t der Mengen A und B oder die P r o d u k t m e n g e von A und B .

Die erste der beiden rechts hingeschriebenen Mengen haben wir nur angegeben, damit nach dem Teilmengenaxiom unmittelbar klar ist, daß $A \times B$ tatsächlich eine Menge ist. Im folgenden wird stets die zweite Form benutzt.

FOLGERUNG:

$$A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$$

Beweis: $A \times B = \emptyset \iff$ es gibt kein Paar (a,b) mit $a \in A \wedge b \in B \iff$ es gibt kein $a \in A$ oder kein $b \in B \iff A = \emptyset \vee B = \emptyset$ .//

Nachdem wir Paare definiert haben, können auch T r i p e l (a,b,c) durch

$$(a,b,c) := ((a,b),c)$$

definiert werden. Dann gilt analog zu den Paaren:

$$(a,b,c) = (x,y,z) \iff a = x \wedge b = y \wedge c = z$$

Beweis: $((a,b),c) = ((x,y),z) \iff (a,b) = (x,y) \wedge c = z \iff a = x \wedge b = y \wedge c = z$, wobei die entsprechende Behauptung für Paare benutzt wurde.

Induktiv lassen sich dann auch n - T u p e l durch

$$(a_1,a_2,\ldots,a_n) := ((a_1,a_2,\ldots,a_{n-1}),a_n)$$

definieren, die wiederum die entsprechende Eigenschaft wie die Paare und Tripel haben. Sind $A_1,\ldots,A_n$ beliebige Mengen, so wird

$$A_1 \times \ldots \times A_n := \{(a_1,\ldots,a_n) \mid a_i \in A_i \ , \ i = 1,\ldots,n\}$$

als die P r o d u k t m e n g e der Mengen $A_1,\ldots,A_n$ bezeichnet. Später, wenn wir Abbildungen zur Verfügung haben, können wir n-Tupel auch als "Familien" definieren (in III. 1.7 und 1.8).

Produktmengen von zwei Mengen spielen im folgenden Kapitel bei der Definition von Relationen eine grundlegende Rolle.

III. Kapitel: Relationen

§ 1 Relationen und Abbildungen

1.1 Definition von Relationen

Die umgangssprachliche Bedeutung des Wortes Relation besagt, daß zwei Objekte, Personen, Begriffe, Ereignisse usw. miteinander in Beziehung stehen. Dieses "in Beziehung stehen" soll nun mathematisch gefaßt werden.

1.1.1 DEFINITION:
Eine R e l a t i o n $\varrho = (A,B,U)$ ist ein Tripel von Mengen A,B,U mit $U \subset A \times B$.

Die Elemente von U sind danach Paare (a,b) mit $a \in A$ und $b \in B$. Man kann die Relation ϱ so interpretieren, daß ein Element $a \in A$ genau dann zu einem Element $b \in B$ in Relation steht, wenn (a,b) in U liegt.

Man nennt eine Relation $\varrho = (A,B,U)$ auch eine Relation von A in B oder von A nach B oder auch zwischen A und B . Ist $A = B$, dann heißt ϱ Relation von A .

1.1.2 BEZEICHNUNGEN:

Q u e l l e von ϱ	$= Qu(\varrho)$	$:= A$
Z i e l von ϱ	$= Zi(\varrho)$	$:= B$
G r a p h von ϱ	$= Gr(\varrho)$	$:= U$
U r b i l d von ϱ	$= Ur(\varrho)$	$:= \{a \mid a \in A \wedge \exists b \in B\,[(a,b) \in U]\}$
B i l d von ϱ	$= Bi(\varrho)$	$:= \{b \mid b \in B \wedge \exists a \in A\,[(a,b) \in U]\}$

1.1.3 BEISPIELE:
1) $\varrho = (A,B,A \times B)$ heißt die größte Relation zwischen A und B ,
2) $\varrho = (A,B,\emptyset)$ heißt die kleinste oder leere Relation zwischen A und B ,
3) $\varrho = (A,A,\{(a,a) \mid a \in A\})$ heißt die identische oder Gleichheitsrelation von A .

Ohne daß wir davon im allgemeinen Fall weiterhin Gebrauch machen, soll noch erwähnt werden, daß für gewisse Relationen eine Produktrelation definiert werden kann. Allerdings wird diese Produktbildung im Spezialfall von Abbildungen bei unseren weiteren Überlegungen eine wichtige Rolle spielen.

1.1.4 DEFINITION:
Gegeben seien Relationen

$$\varrho = (A,B,U) \quad , \qquad \sigma = (B,C,V) \; .$$

Dann heißt

$$\sigma\varrho := (A,C,W)$$

mit

$$W := \{(a,c) \mid (a,c) \in A \times C \wedge \exists b \in B \, [(a,b) \in U \wedge (b,c) \in V]\}$$

die P r o d u k t r e l a t i o n von ϱ und σ .

Man beachte, daß hierbei $Zi(\varrho) = Qu(\sigma)$ vorausgesetzt wurde.

Im folgenden werden drei Typen von Relationen eingehend betrachtet und zwar Abbildungen, Äquivalenzrelationen und Ordnungen.

1.2 Einführung in den Begriff der Abbildung

In der klassischen Mathematik treten Abbildungen vor allem als Funktionen, als Abbildungen der Geometrie und als Permutationen auf. In dieser Weise kommen Abbildungen auch bereits in der Schulmathematik vor. Insbesondere ist bekannt, daß reelle (oder auch komplexe) Funktionen dazu dienen, inner- und außermathematische Zusammenhänge und Vorgänge darzustellen. Beispiele für solche Funktionen sind aus der Schule bekannt wie etwa die rationalen Funktionen, die trigonometrischen Funktionen, die Exponentialfunktion und der Logarithmus. Für die geometrischen Abbildungen hat man Beispiele in den Projektionen, den Spiegelungen und Drehungen. Schließlich versteht man im klassischen Sinne unter einer Permutation etwa der Zahlen 1,2,3,4 eine Anordnung dieser Zahlen in einer bestimmten Reihenfolge wie etwa 2,1,4,3 oder 4,1,3,2 .

Derartige Abbildungen wurden früher meist durch eine "Zuordnungsvorschrift" oder eine Gleichung erklärt , ohne daß genau definiert wurde, was etwa eine "Zuordnungsvorschrift" ist. Das Bedürfnis nach einer mathematisch präzisen und allgemeinen Definition der Abbildung wurde durch den auf der Mengenlehre beruhenden modernen Abbildungsbegriff befriedigt. Dieser entstand erst zu Beginn dieses Jahrhunderts. In der Folgezeit hat er sich rasch über seine frühere Bedeutung hinaus zu einem der fundamentalen Begriffe der Mathematik entwickelt. Dabei sind drei mehr oder weniger zusammenhängende Gesichtspunkte in den Vordergrund gerückt.

1. GESICHTSPUNKT:
Sind mathematische Objekte gleicher Struktur gegeben, so werden "strukturerhaltende" Abbildungen zwischen ihnen betrachtet. Diese übertragen Eigenschaften eines Objektes auf andere Objekte gleicher Struktur. Diese Abbildungen stellen gewissermaßen ein technisches Hilfsmittel zur Untersuchung entsprechender Objekte dar. Beispiele hierfür werden wir später in den Gruppenhomomorphismen, den Ringhomomorphismen, den linearen Abbildungen von Vektorräumen sowie den stetigen Abbildungen und Homöomorphismen von topologischen Räumen kennenlernen.

2. GESICHTSPUNKT:
Man stellt fest, daß gewisse Mengen von strukturerhaltenden Abbildungen selbst wieder eine interessante Struktur besitzen können. Diese Mengen von Abbildungen mit der entsprechenden Struktur werden dann zum Gegenstand der Untersuchung gemacht. Dafür werden wir später Beispiele kennen lernen wie etwa die Automorphismengruppe einer Gruppe, den Ring der Endomorphismen eines Vektorraums und den dualen Vektorraum.

3. GESICHTSPUNKT:
In der jüngsten Entwicklung hat sich gezeigt, daß oftmals nicht die ursprünglichen mathematischen Objekte an sich von primärer Bedeutung sind, sondern die strukturerhaltenden Abbildungen, die zwischen Objekten gleicher Struktur bestehen. Das kann so weit gehen, daß die Objekte ganz in den Hinter-

grund treten und es nur noch auf die Abbildungen ankommt, da diese wesentliche Informationen über die Objekte mitenthalten. Eine Ausprägung hat dieser Gesichtspunkt, der mit den beiden erstgenannten Gesichtspunkten eng zusammenhängt, im Begriff der Kategorie gefunden. Darauf gehen wir im VI.Kapitel ein.

1.3 Abbildungen, Definition und Beispiele

1.3.1 DEFINITION:
Eine Relation $\alpha = (A,B,U)$ heißt A b b i l d u n g , F u n k t i o n oder F a m i l i e , wenn gilt:
(1) $\forall a \in A \; \exists b \in B \; [(a,b) \in U]$
(2) $\forall a \in A \; \forall b_1, b_2 \in B \; [(a,b_1) \in U \wedge (a,b_2) \in U \Longrightarrow b_1 = b_2]$.
Benutzt man für α die Bezeichnung Familie, dann heißt A die Indexmenge von α . α heißt auch Abbildung von A nach B .

Die Bedingungen (1) und (2) zusammen können wie folgt ausgedrückt werden: Zu jedem $a \in A$ existiert genau ein $b \in B$ mit $(a,b) \in U$.

Bei Abbildungen benutzen wir die allgemein für Relationen eingeführten Bezeichnungen. Da jetzt jedoch nach Definition der Abbildung $Ur(\alpha) = A = Qu(\alpha)$ gilt, ist die Bezeichnung $Ur(\alpha)$ überflüssig.

Das durch ein $a \in A$ bei der Abbildung α eindeutig bestimmte Element $b \in B$ mit $(a,b) \in Gr(\alpha)$ bezeichnet man mit $\alpha(a)$; folglich gilt dann für beliebige $a \in A$ und $b \in B$:

$$(\alpha(a) = b) \Longleftrightarrow ((a,b) \in Gr(\alpha)) .$$

Eine weitere Bezeichnungsweise für $\alpha(a) = b$ ist auch $a \overset{\alpha}{\longmapsto} b$ oder einfach $a \longmapsto b$ mit der Sprechweise "dem Element a wird durch α das Element b zugeordnet". Man nennt b auch das B i l d von a bei α und a ein U r b i l d von b bei α . Schließlich sagt man auch, daß a auf b bei α abgebildet wird. Die Abbildung α wird auch durch die Schreibweise

$$\alpha : A \longrightarrow B \quad \text{oder} \quad A \overset{\alpha}{\longrightarrow} B$$

angegeben. Nicht ganz korrekt aber bequem schreiben wir auch

$$\alpha: \quad A \ni a \longmapsto b \in B \quad ,$$

wobei oft auch noch α weggelassen wird. Statt dem Bild b von a gibt man häufig auch eine Formel an, mit der b aus a berechnet werden kann (falls eine solche Situation vorliegt).

Man beachte den Unterschied im Gebrauch der beiden Pfeile $\longrightarrow$ und $\longmapsto$. Der Pfeil $\longrightarrow$ wird dann verwendet, wenn links und rechts davon die Mengen stehen, zwischen denen die Abbildung definiert ist. Der Pfeil $\longmapsto$ wird verwendet, wenn links und rechts davon Elemente stehen, die bei der Abbildung einander zugeordnet werden. Diese Konvention ist besonders dann genau zu beachten, wenn die Elemente selbst Mengen sind, also zum Beispiel bei Abbildungen zwischen Potenzmengen.

Es soll noch einmal ausdrücklich darauf hingewiesen werden, daß die Sprechweise "a wird durch α das Element b zugeordnet" keine inhaltliche Bedeutung hat, sondern nur die, daß $(a,b) \in Gr(\alpha)$ gilt.

Zwei Abbildungen α und β sind nach Definition genau dann gleich, wenn die Tripel $(Qu(\alpha),Zi(\alpha),Gr(\alpha))$ und $(Qu(\beta),Zi(\beta),Gr(\beta))$ gleich sind, also wenn gilt

$$Qu(\alpha) = Qu(\beta) \wedge Zi(\alpha) = Zi(\beta) \wedge \forall a \in Qu(\alpha)\,[\alpha(a) = \beta(a)] \quad .$$

1.3.2 DEFINITION:

1) Die Abbildung $\alpha = (A,B,U)$ heißt s u r j e k t i v oder eine S u r j e k t i o n oder Abbildung von A a u f B:

$$\Longleftrightarrow \quad \forall b \in B\, \exists a \in A\,[(a,b) \in U] \quad ,$$

das heißt, alle Elemente aus dem Ziel von α sind Bilder von Elementen aus der Quelle von α, also $Bi(\alpha) = Zi(\alpha)$.

2) Die Abbildung $\alpha = (A,B,U)$ heißt i n j e k t i v oder eine I n j e k t i o n oder eine e i n e i n d e u t i g e Abbildung:

$$\Longleftrightarrow \quad \forall b \in B\, \forall a_1,a_2 \in A\,[(a_1,b) \in U \wedge (a_2,b) \in U \Rightarrow a_1 = a_2],$$

das heißt, je zwei verschiedene Elemente aus A werden auf verschiedene Elemente aus B abgebildet.

3) Die Abbildung $\alpha = (A,B,U)$ heißt b i j e k t i v oder eine B i j e k t i o n : $\Longleftrightarrow$ α ist surjektiv und injektiv.

Sei nun $\alpha = (A,B,U)$ eine bijektive Abbildung, dann setze man

$$U' := \{(b,a) \mid (b,a) \in B \times A \wedge (a,b) \in U\} .$$

1.3.3 FOLGERUNG:
Ist $\alpha = (A,B,U)$ eine bijektive Abbildung und sei U' wie zuvor definiert, dann ist $\alpha' = (B,A,U')$ ebenfalls eine bijektive Abbildung.

Beweis: Nach Definition von α' ist klar, daß dies eine Relation ist. Da α surjektiv ist, ist die Bedingung (1) in 1.3.1 für α' erfüllt. Da α injektiv ist, ist die Bedingung (2) in 1.3.1 für α' erfüllt. Folglich ist α' eine Abbildung. Aus der Bedingung 1.3.1 (1) für α folgt, daß α' surjektiv ist. Schließlich folgt aus der Bedingung 1.3.1 (2) für α, daß α' injektiv ist.//

1.3.4 BEISPIELE:

1) Die i d e n t i s c h e Abbildung einer Menge A, bezeichnet mit 1_A

$$1_A : A \ni a \longmapsto a \in A .$$

Offenbar ist dies die identische Relation (siehe 1.1.3), die jetzt als identische Abbildung bezeichnet wird.

2) $\mathbb{N} \ni n \longmapsto 2n \in \mathbb{N}$.

3) $\mathbb{N} \ni n \longmapsto 2n \in \{2,4,6,8,\ldots\}$.

Man beachte, daß die Abbildungen in 2) und 3) verschieden sind, da ihre Ziele verschieden sind. Die Abbildung in 2) ist injektiv, aber nicht surjektiv, während die Abbildung in 3) bijektiv ist.

4) $\mathbb{R} \ni r \longmapsto [r] \in \mathbb{Z}$.

Dabei sei $[r]$ die größte ganze Zahl $\leq r$. Diese Abbildung ist surjektiv aber nicht injektiv.

5) $\mathbb{Q} \ni q \longmapsto q \in \mathbb{R}$,

dies ist die I n k l u s i o n s a b b i l d u n g der Teilmenge $\mathbb{Q} \subset \mathbb{R}$ in $\mathbb{R}$. Diese Abbildung, die von $1_{\mathbb{Q}}$ verschieden ist, ist injektiv aber nicht surjektiv.

6) $\mathbb{R} \ni r \longmapsto 2^r \in \mathbb{R}^+$,

$\mathbb{R}^+ := \{ r \mid r \in \mathbb{R} \wedge r > 0 \}$.

In gewissen Situationen möchte man eine Abbildung nur für eine Teilmenge der Quelle der Abbildung betrachten. Man spricht dann von einer Einschränkung der Abbildung.

1.3.5 DEFINITION:
Sei $\alpha : A \longrightarrow B$ eine Abbildung und sei $A_0 \subset A$, dann heißt

$$\alpha|A_0 := (A_0, B, Gr(\alpha) \cap (A_0 \times B))$$

die E i n s c h r ä n k u n g von α auf A_0 .

Es ist sofort zu sehen, daß $\alpha|A_0$ wieder eine Abbildung ist. Gelegentlich ist es auch zweckmäßig, daß Ziel B von α einzuschränken, allerdings nur zu einer Teilmenge von B , die noch das Bild von α enthält.

1.4 Eine Kennzeichnung endlicher Mengen

Für eine Abbildung einer endlichen Menge in sich fallen die Begriffe surjektiv, injektiv und bijektiv zusammen. Dies ist in der folgenden Behauptung enthalten.

1.4.1 BEHAUPTUNG:
Seien A und B zwei Mengen mit je n Elementen (mit $n \in \mathbb{N}$). Dann sind für eine Abbildung $\alpha : A \longrightarrow B$ äquivalent:

(1) α ist surjektiv
(2) α ist injektiv
(3) α ist bijektiv

Beweis:
(1) $\Longrightarrow$ (2): Seien $b_1, \ldots, b_n$ die Elemente aus B . Da α

surjektiv ist, ist jedes Element b_i Bild (mindestens) eines Elementes a_i bei α, also $\alpha(a_i) = b_i$ für $i = 1,\ldots,n$. Da α eine Abbildung ist, sind die Elemente $a_1,\ldots,a_n$ alle voneinander verschieden und daher genau alle Elemente aus A. $\alpha(a_i) = b_i$ besagt dann, daß verschiedene Elemente aus A verschiedene Bilder besitzen, also ist α injektiv.
(2) $\Rightarrow$ (3): Es genügt zu zeigen, daß α auch surjektiv ist. Da α injektiv ist, haben die n verschiedenen Elemente aus A auch n verschiedene Bildelemente. Da B nur n Elemente enthält, sind die Bildelemente alle Elemente aus B, also ist α surjektiv.
(3) $\Rightarrow$ (1): Gilt nach Definition von bijektiv. //

Wir sind jetzt in der Lage, die Endlichkeit einer Menge durch Abbildungen zu Kennzeichnen. Bei einem axiomatischen Aufbau kann diese Kennzeichnung zur Definition der Endlichkeit einer Menge benutzt werden.

1.4.2 SATZ:
Für eine Menge A sind folgende Eigenschaften äquivalent:

(1) A ist endlich ,
(2) jede surjektive Abbildung von A nach A ist bijektiv ,
(3) jede injektive Abbildung von A nach A ist bijektiv.

Beweis:
(1) $\Rightarrow$ (2) $\wedge$ (3): Folgt aus 1.4.1.
(2) $\Rightarrow$ (1) $\wedge$ (3) $\Rightarrow$ (1): Zum Beweis benutzen wir das Kontrapositionsgesetz (I.1.4, Tautologie 40)). Danach muß gezeigt werden, daß es zu einer unendlichen Menge A stets eine surjektive Abbildung und eine injektive Abbildung gibt, die nicht bijektiv sind. Wir können dies zeigen, wenn wir benutzen, daß eine unendliche Menge A stets eine unendliche abzählbare Teilmenge

$$N = \{ a_1, a_2, a_3, \ldots \mid a_i \neq a_j \text{ für } i \neq j \}$$

besitzt. Sei die Abbildung $\alpha : A \longrightarrow A$ folgendermaßen definiert:

$$\alpha(a) := a \qquad \text{für} \quad a \in A \setminus N$$
$$\alpha(a_{2i}) := a_i \qquad \text{für} \quad i \in \mathbb{N}$$
$$\alpha(a_{2i-1}) := a_1 \qquad \text{für} \quad i \in \mathbb{N} \ ,$$

dann ist α surjektiv aber nicht injektiv, da alle a_{2i-1} das gleiche Bild a_1 haben. Setzt man stattdessen

$$\alpha(a) := a \qquad \text{für} \quad a \in A \setminus N$$
$$\alpha(a_i) := a_{2i} \qquad \text{für} \quad i \in \mathbb{N} \ ,$$

dann ist α injektiv aber nicht surjektiv, da die Elemente a_{2i-1} , $i \in \mathbb{N}$ nicht in $Bi(\alpha)$ enthalten sind.//

1.5 Produkte von Abbildungen

Gegeben seien jetzt zwei Abbildungen

$$\alpha : A \longrightarrow B \quad , \qquad \beta : B \longrightarrow C \quad ,$$

wobei also $Zi(\alpha) = Qu(\beta)$ ist. Dann kann als Spezialfall von 1.1.4 das Produkt $\beta\alpha$ definiert werden.

1.5.1 DEFINITION:
Mit den vorstehenden Abbildungen α und β sei

$$\beta\alpha := (A,C,W)$$

mit

$$W := \{(a,\beta(\alpha(a))) \mid a \in A\} \ ,$$

so daß also

$$\beta\alpha(a) = \beta(\alpha(a)) \qquad \text{für} \quad a \in A$$

gilt. $\beta\alpha$ heißt das P r o d u k t oder die H i n t e r e i n a n d e r a u s f ü h r u n g der Abbildungen α und β.

Offensichtlich ist die Relation $\beta\alpha = (A,C,W)$ wieder eine Abbildung, denn zu jedem $a \in A$ ist $\beta(\alpha(a))$ ein durch a eindeutig bestimmtes Element aus C , denn nach Voraussetzung sind $\alpha(a)$ durch a und $\beta(\alpha(a))$ durch $\alpha(a)$ eindeutig bestimmt.

Wir weisen noch einmal ausdrücklich darauf hin, daß $\beta\alpha$ nur unter der Voraussetzung $Zi(\alpha) = Qu(\beta)$ definiert ist und wollen dies bei der Schreibweise $\beta\alpha$ stets voraussetzen.

1.5.2 FOLGERUNG:
"Kategorische Eigenschaften" des Produktes von Abbildungen.

1) Seien $\alpha : A \longrightarrow B$, $\beta : B \longrightarrow C$, $\gamma : C \longrightarrow D$ Abbildungen, dann gilt das a s s o z i a t i v e G e s e t z : $\gamma(\beta\alpha) = (\gamma\beta)\alpha$.

2) Für die schon eingeführte identische Abbildung 1_A bzw. 1_B gilt: $\alpha = \alpha 1_A = 1_B \alpha$.

Beweis:

1): Quelle (= A) und Ziel (= D) von $\gamma(\beta\alpha)$ und $(\gamma\beta)\alpha$ stimmen offensichtlich überein. Fragt sich nur, ob im Graphen beider Abbildungen zu $a \in A$ jeweils die gleiche zweite Komponente aus D gehört. Für $\gamma(\beta\alpha)$ ist diese nach Definition des Produktes gleich

$$(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$$

und für $(\gamma\beta)\alpha$ gleich

$$((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a))) \quad .$$

Also gilt die Behauptung.

2): Quelle (= A) und Ziel (= B) von α , $\alpha 1_A$ und $1_B \alpha$ stimmen überein. Da auch

$$\alpha(a) = \alpha(1_A(a)) = 1_B(\alpha(a))$$

gilt, folgt 2).//

Die Bezeichnung "kategorische Eigenschaften" wird erst im VI. Kapitel erläutert, doch soll hier bereits erwähnt werden, daß es sich dabei um die definierenden Eigenschaften einer Kategorie handelt. So bildet die Klasse aller Mengen zusammen mit allen Abbildungen von Mengen die Kategorie der Mengen.

Mit Hilfe des Produktes kann man surjektive und injektive Abbildungen in folgender Weise kennzeichnen.

1.5.3 SATZ:
Für eine Abbildung $\alpha : A \longrightarrow B$ gilt :

1) α ist dann und nur dann surjektiv, wenn für beliebige Abbildungen β_1, β_2 gilt:

$$\beta_1\alpha = \beta_2\alpha \quad \Longrightarrow \quad \beta_1 = \beta_2 \ .$$

2) α ist dann und nur dann injektiv, wenn für beliebige Abbildungen γ_1, γ_2 gilt:

$$\alpha\gamma_1 = \alpha\gamma_2 \quad \Longrightarrow \quad \gamma_1 = \gamma_2$$

Beweis: Bei der Formulierung des Satzes haben wir die zuvor eingeführte Konvention benutzt, daß die Schreibweise $\beta\alpha$ die Voraussetzung $Zi(\alpha) = Qu(\beta)$ einschließen soll.

1): Sei α surjektiv und gelte $\beta_1\alpha = \beta_2\alpha$, dann folgt zunächst

$$Zi(\beta_1) = Zi(\beta_1\alpha) = Zi(\beta_2\alpha) = Zi(\beta_2) \ ,$$

$$B = Zi(\alpha) = Qu(\beta_1) = Qu(\beta_2) \ .$$

Sei jetzt $b \in B$, dann gibt es, da α surjektiv ist, ein $a \in A$ mit $\alpha(a) = b$. Nach Voraussetzung folgt dann

$$\beta_1(b) = \beta_1(\alpha(a)) = \beta_1\alpha(a) = \beta_2\alpha(a) = \beta_2(\alpha(a)) = \beta_2(b) \ ,$$

also gilt auch $Gr(\beta_1) = Gr(\beta_2)$ und folglich $\beta_1 = \beta_2$.
Um die Umkehrung zu beweisen, zeigen wir, daß für eine nicht surjektive Abbildung α die Bedingung in 1) nicht erfüllt ist. Sei also α nicht surjektiv, dann gibt es ein Element $b_0 \in B$ mit $b_0 \notin Bi(\alpha)$. Seien nun Abbildungen

$$\beta_i \ : \ B \longrightarrow \{1,2\} \quad , \quad i = 1,2$$

definiert durch

$$\beta_1(b) := 1 \quad \text{für alle} \quad b \in B \ ,$$

$$\beta_2(b) := \begin{cases} 1 & \text{für} \quad b \in B \wedge b \neq b_0 \\ 2 & \text{für} \quad b = b_0 \end{cases} \ .$$

Dann gilt $\beta_1 \neq \beta_2$; da b_0 nicht in $Bi(\alpha)$ enthalten ist, gilt andererseits für alle $a \in A$

$$\beta_1\alpha(a) = \beta_1(\alpha(a)) = \beta_2(\alpha(a)) = \beta_2\alpha(a) \ ,$$

also $\beta_1\alpha = \beta_2\alpha$.

2): Sei α jetzt injektiv und gelte $\alpha\gamma_1 = \alpha\gamma_2$, dann folgt zunächst

$$Qu(\gamma_1) = Qu(\alpha\gamma_1) = Qu(\alpha\gamma_2) = Qu(\gamma_2) \quad ,$$

$$A = Qu(\alpha) = Zi(\gamma_1) = Zi(\gamma_2) \quad .$$

Für $c \in Qu(\gamma_1) = Qu(\gamma_2)$ gilt nach Voraussetzung

$$\alpha(\gamma_1(c)) = \alpha\gamma_1(c) = \alpha\gamma_2(c) = \alpha(\gamma_2(c))$$

und da α injektiv ist, folgt $\gamma_1(c) = \gamma_2(c)$, woraus sich $Gr(\gamma_1) = Gr(\gamma_2)$ ergibt. Also gilt $\gamma_1 = \gamma_2$. Um die Umkehrung zu zeigen, sei α nicht injektiv, das heißt, es gebe Elemente $a_1, a_2 \in A$, $a_1 \neq a_2$ mit $\alpha(a_1) = \alpha(a_2)$. Dann betrachte man die Abbildungen

$$\gamma_i : \{1\} \longrightarrow A \quad , \quad i = 1,2$$

$$\gamma_1(1) := a_1 \quad , \quad \gamma_2(1) := a_2 \quad .$$

Dann gilt $\gamma_1 \neq \gamma_2$; andererseits folgt

$$\alpha\gamma_1(1) = \alpha(a_1) = \alpha(a_2) = \alpha\gamma_2(1) \quad ,$$

also $\alpha\gamma_1 = \alpha\gamma_2$. Damit ist auch 2) bewiesen.//

Für spätere Verwendung zeigen wir jetzt noch den folgenden Hilfssatz.

1.5.4 HILFSSATZ:
Seien $\alpha : A \longrightarrow B$ und $\beta : B \longrightarrow C$ Abbildungen, dann gilt:

1) Surjektiv $\alpha \wedge$ surjektiv $\beta \implies$ surjektiv $\beta\alpha$,
   injektiv $\alpha \wedge$ injektiv $\beta \implies$ injektiv $\beta\alpha$.

2) Surjektiv $\beta\alpha \implies$ surjektiv β ,
   injektiv $\beta\alpha \implies$ injektiv α .

Beweis:
1): Folgt sofort aus der Definition von surjektiv und injektiv.
2): Surjektiv $\beta\alpha \implies Bi(\beta\alpha) = Zi(\beta\alpha) = Zi(\beta)$. Da

$$Bi(\beta\alpha) = \{(\beta(a)) \mid a \in A\} \subset Bi(\beta) = \{\beta(b) \mid b \in B\}$$

folgt $Bi(\beta) = Zi(\beta)$, das heißt, β ist surjektiv. Zum Beweis der zweiten Behauptung seien $a_1, a_2 \in A$ und $a_1 \neq a_2$, dann folgt nach Voraussetzung

$$\beta(\alpha(a_1)) = \beta\alpha(a_1) \neq \beta\alpha(a_2) = \beta(\alpha(a_2)) \quad ,$$

also auch $\alpha(a_1) \neq \alpha(a_2)$, das heißt, α ist injektiv.//

1.6 Inverse Abbildungen

Es soll jetzt festgestellt werden, daß es zu bijektiven Abbildungen (beidseitige) Umkehrabbildungen gibt.

1.6.1 HILFSSATZ:
Für die Abbildung $\alpha : A \longrightarrow B$ gilt:
Dann und nur dann ist α bijektiv, wenn eine Abbildung

$$\alpha' : B \longrightarrow A \quad \text{mit} \quad \alpha'\alpha = 1_A \quad \text{und} \quad \alpha\alpha' = 1_B$$

existiert.

Beweis:
"$\Longrightarrow$": Sei jetzt $\alpha = (A,B,U)$ bijektiv. Für α' wähle man die in 1.3.3 angegebene Bijektion $\alpha' = (B,A,U')$. Aus der Definition von diesem α' folgt dann sofort $\alpha'\alpha = 1_A$ und $\alpha\alpha' = 1_B$.
"$\Longleftarrow$": Da 1_A und 1_B beide bijektiv sind, folgt nach Voraussetzung und 1.5.4, daß α surjektiv und injektiv also bijektiv ist.//

Ergänzend zu diesem Hilfssatz stellen wir noch fest, daß zu bijektivem α nur genau ein α' mit $\alpha'\alpha = 1_A$ und $\alpha\alpha' = 1_B$ existiert. Sei auch $\beta : B \longrightarrow A$ eine solche Abbildung, dann folgt

$$\alpha' = \alpha' 1_B = \alpha'(\alpha\beta) = (\alpha'\alpha)\beta = 1_A\beta = \beta ,$$

wobei wir von α' nur $\alpha'\alpha = 1_A$ und von β nur $\alpha\beta = 1_B$ benutzt haben.

1.6.2 DEFINITION:
Sei $\alpha : A \longrightarrow B$ bijektiv. Dann wird die zuvor mit α' bezeichnete Abbildung

$$\alpha' = (B,A,U') \quad \text{mit} \quad U' = \{(b,a) \mid (a,b) \in Gr(\alpha)\}$$

die zu α i n v e r s e A b b i l d u n g genannt und mit α^{-1} bezeichnet.

1.6.3 FOLGERUNG:

1) Bijektiv $\alpha \Longrightarrow$ bijektiv $\alpha^{-1} \wedge (\alpha^{-1})^{-1} = \alpha$.

2) Bijektiv $\alpha \wedge$ bijektiv $\beta \wedge Zi(\alpha) = Qu(\beta)$
$\Rightarrow$ bijektiv $\beta\alpha \wedge (\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$.

Beweis:
1): Nach 1.3.3 ist α^{-1} bijektiv. Da in 1.6.1 die Bedingung

$$\alpha'\alpha = 1_A \quad , \quad \alpha\alpha' = 1_B$$

symmetrisch in α und $\alpha' = \alpha^{-1}$ ist, ist α die zu α^{-1} inverse Abbildung, die der Bezeichnung entsprechend als $(\alpha^{-1})^{-1}$ geschrieben wird, daß heißt, es gilt $\alpha = (\alpha^{-1})^{-1}$. Dabei wird die zuvor festgestellte Eindeutigkeit der inversen Abbildung benutzt.
2): Es gilt

$$\begin{aligned}(\alpha^{-1}\beta^{-1})(\beta\alpha) &= \alpha^{-1}(\beta^{-1}\beta)\alpha \\ &= \alpha^{-1}1_B\alpha = \alpha^{-1}\alpha = 1_A\end{aligned}$$

sowie entsprechend

$$(\beta\alpha)(\alpha^{-1}\beta^{-1}) = 1_C \quad (\text{mit } C = Zi(\beta)) .$$

Auf Grund von 1.6.1 und der Eindeutigkeit der inversen Abbildung folgt auch jetzt die Behauptung.//

Man beachte in diesem Zusammenhang, daß für eine Abbildung $\alpha : A \longrightarrow B$ aus der Existenz einer Abbildung $\beta : B \longrightarrow A$ mit $\beta\alpha = 1_A$ keineswegs auch $\alpha\beta = 1_B$, also die Bijektivität von α folgen muß. Sei zum Beispiel

$$\alpha : \mathbb{N} \ni n \longmapsto 2n \in \mathbb{N}$$

und sei $\beta : \mathbb{N} \longrightarrow \mathbb{N}$ mit

$$\beta(2n) := n \quad , \quad \beta(2n-1) := 1 \quad ,$$

dann gilt offenbar

$$\beta\alpha = 1_{\mathbb{N}} \qquad \text{aber} \quad \alpha\beta \neq 1_{\mathbb{N}} \quad ,$$

denn $\alpha\beta(2n-1) = \alpha(1) = 2$.

1.7 Familien

Nach Definition 1.3.1 besteht sachlich kein Unterschied zwischen Abbildungen und Familien. Es handelt sich um zwei verschiedene Bezeichnungen für den gleichen Begriff. Dennoch wird ein gewisser Unterschied im Gebrauch dieser beiden Bezeichnungen gemacht. Recht vage kann man sagen, daß man

die Bezeichnung Familie benutzt, wenn es vor allem auf die Bilder ankommt oder wenn die Indexmenge (= Quelle) der Familie total geordnet ist (siehe dazu 3.2) und diese Ordnung eine Rolle spielt (wie zum Beispiel bei der Konvergenz von Folgen).

Ist $f : \mathfrak{J} \longrightarrow M$ eine Familie, dann wird für f meist eine der folgenden Schreibweisen benutzt:

$$f = (f(i) \mid i \in \mathfrak{J}) = (f(i)) = (f_i \mid i \in \mathfrak{J}) = (f_i)$$
$$= (m_i) \quad (\text{mit } m_i = f(i)) .$$

Man nennt f eine Familie zur Indexmenge $\mathfrak{J}$ mit Koeffizienten in M . Ist $\mathfrak{J} = \{1,2,\ldots,n\}$, dann wird auch

$$f = (f_1,f_2,\ldots,f_n) \quad (\text{mit } f_i = f(i))$$

geschrieben. Ist $\mathfrak{J} = \mathbb{N}$, dann schreibt man

$$f = (f_1,f_2,f_3,\ldots) = (f_i)$$

und f heißt dann eine F o l g e von Elementen aus M .

1.8 Beliebige Produktmengen

Der aufmerksame Leser wird bei der soeben eingeführten Schreibweise für Familien irritiert sein, denn die Symbole $(a_1,\ldots,a_n)$, speziell (a,b) und (a,b,c) hatten wir bereits in II.2 mit anderer Bedeutung eingeführt. Dort waren es die Elemente entsprechender Produktmengen. Daß man den Unterschied in der Bedeutung tatsächlich ignorieren kann, soll hier auseinandergesetzt werden.

Zu zwei beliebigen Mengen A und B hatten wir in II.2.2 die Produktmenge

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$$

definiert. Es soll jetzt eine Menge von Familien angegeben werden, die zu $A \times B$ bijektiv ist, so daß wir damit - bis auf eine Bijektion - eine neue Definition für $A \times B$ erhalten haben. Sei

$$f : \{1,2\} \longrightarrow A \cup B$$

mit $f(1) \in A \wedge f(2) \in B$.

Bezeichne $A \not\times B$ die Menge aller solchen Familien.

1.8.1 BEHAUPTUNG:

$$\Phi : A \not\times B \ni f \longrightarrow (f(1),f(2)) \in A \times B$$

ist eine Bijektion.

Beweis: Zu beliebigen $a \in A$ und $b \in B$ sei

$$f : \{1,2\} \longrightarrow A \cup B$$

definiert durch

$$f(1) := a \quad , \quad f(2) := b \quad .$$

Dann folgt $\Phi(f) = (f(1),f(2)) = (a,b)$, also ist Φ surjektiv. Seien jetzt $f,g \in A \not\times B$ mit

$$\Phi(f) = (f(1),f(2)) = (g(1),g(2)) = \Phi(g) \quad ,$$

dann folgt

$$f(1) = g(1) \quad , \quad f(2) = g(2) \quad ,$$

also $f = g$, das heißt, Φ ist auch injektiv.//

Nachdem man weiß, daß Φ eine Bijektion ist, läßt man den Unterschied in der Schreibweise $A \not\times B$ und $A \times B$ weg und schreibt in beiden Fällen $A \times B$, sowie für die Elemente $(f(1),f(2))$ oder (f_1,f_2) mit $f_1 = f(1)$, $f_2 = f(2)$. Welche Definition dabei zugrunde gelegt wird, kann dem jeweiligen Zweck überlassen bleiben.

Entsprechend kann man auch, wenn die Mengen $A_1,\ldots,A_n$ gegeben sind, als $A_1 \not\times A_2 \not\times \ldots \not\times A_n$ die Menge aller Familien

$$f : \{1,2,\ldots,n\} \longrightarrow A_1 \cup A_2 \cup \ldots \cup A_n$$

mit

$$f(i) \in A_i \quad \text{für} \quad i = 1,2,\ldots,n$$

definieren. Wie zuvor für $n = 2$ sieht man auch jetzt, daß die Menge $A_1 \not\times A_2 \not\times \ldots \not\times A_n$ zur Menge $A_1 \times A_2 \times \ldots \times A_n$ bijektiv ist und zwar mit der Bijektion

$$A_1 \not\times \ldots \not\times A_n \ni f \longmapsto (f(1),\ldots,f(n)) \in A_1 \times \ldots \times A_n \quad .$$

Auch jetzt schreibt man für beide Mengen $A_1 \times \ldots \times A_n$ und identifiziert f mit $(f(1),\ldots,f(n))$, wie wir das schon im

vorhergehenden Abschnitt allgemein als Bezeichnung bei Familien eingeführt haben.

Die neue Auffassung trägt allerdings weiter, da man jetzt nicht auf endliche Indexmengen beschränkt ist.

1.8.2 DEFINITION:
Sei $\{A_i \mid i \in \mathfrak{J}\}$ eine Menge, bei der die Elemente A_i selbst wieder Mengen sind. Die Menge aller Familien

$$f : \mathfrak{J} \longrightarrow \bigcup_{i\in\mathfrak{J}} A_i \quad \text{mit} \quad f(i) \in A_i \quad \text{für alle} \quad i \in \mathfrak{J}$$

heißt das P r o d u k t der Mengen A_i, $i \in \mathfrak{J}$, bezeichnet mit

$$\prod_{i\in\mathfrak{J}} A_i \quad .$$

Die Voraussetzung, daß $\{A_i \mid i \in \mathfrak{J}\}$ eine Menge ist, wird gebraucht, damit nach II.1.4, Axiom (M 4) sichergestellt ist, daß $\bigcup_{i\in\mathfrak{J}} A_i$ existiert.

Schreibt man $f = (f(i)) = (f_i)$, so folgt

$$\prod_{i\in\mathfrak{J}} A_i = \{(f(i)) \mid \forall i \in \mathfrak{J}\, [f(i) \in A_i]\}$$

oder kurz

$$\prod_{i\in\mathfrak{J}} A_i = \{(f_i) \mid f_i \in A_i\} \quad .$$

Man beachte bei dieser Definition, daß für die Menge $\{A_i \mid i \in \mathfrak{J}\}$ nicht notwendig $A_i \neq A_j$ für $i \neq j$ gelten muß. Zum Beispiel ist darin auch der Fall

$$A_i = A \quad \text{für alle} \quad i \in \mathfrak{J}$$

enthalten. Das Produkt hängt also tatsächlich nicht nur von der Menge $\{A_i \mid i \in \mathfrak{J}\}$, sondern auch von der Indexmenge $\mathfrak{J}$ ab, die angibt "wieviel" Faktoren vorkommen. Es ist daher vielleicht klarer, das Produkt nicht zu der "indizierten Menge" $\{A_i \mid i \in \mathfrak{J}\}$ von Mengen, sondern zu der folgenden Familie zu definieren. Sei

$$A := \bigcup_{i\in\mathfrak{J}} A_i$$

und sei $P = P(A)$ die Potenzmenge von A. Die Familie

$$\alpha : \mathfrak{J} \longrightarrow P$$

sei dann durch

$$\alpha(i) = A_i \quad \text{für alle} \quad i \in \mathfrak{J}$$

definiert. In der von uns eingeführten Schreibweise ist

$$\alpha = (A_i \mid i \in \mathfrak{J}) .$$

Durch diese Familie von Mengen sind die Bestimmungsstücke zur Definition von $\prod_{i \in \mathfrak{J}} A_i$ genau angegeben.

Im Falle

$$A_i = A \quad \text{für alle} \quad i \in \mathfrak{J}$$

wird

$$A^{\mathfrak{J}} := \prod_{i \in \mathfrak{J}} A_i$$

gesetzt. Man bezeichnet $A^{\mathfrak{J}}$ auch als Produkt von $\mathfrak{J}$ Kopien der Menge A . Mit anderen Worten: $A^{\mathfrak{J}}$ ist die Menge aller Abbildungen von $\mathfrak{J}$ nach A .

1.9 Induzierte Abbildungen auf Potenzmengen

Seien A und B Mengen, und sei $\alpha : A \longrightarrow B$ eine Abbildung. Durch α werden zwischen den Potenzmengen P(A) und P(B) zwei Abbildungen induziert. Die eine Abbildung ist definiert durch

$$\alpha_p : P(A) \ni X \longrightarrow \{b \mid b \in B \wedge \exists x \in X [f(x) = b]\} \in P(B) .$$

$\alpha_p(X)$ wird häufig das Bild von X bei α genannt und kurz mit

$$\alpha_p(X) = \{\alpha(x) \mid x \in X\}$$

bezeichnet. Die zweite Abbildung ist definiert durch .

$$\alpha^p : P(B) \ni Y \longrightarrow \{a \mid a \in A \wedge f(a) \in Y\} \in P(A) .$$

$\alpha^p(Y)$ wird auch als Urbild von Y bei α bezeichnet.

In der Literatur findet man statt $\alpha_p(X)$ auch häufig die Schreibweise $\alpha(X)$ und statt $\alpha^p(Y)$ die Schreibweise $\alpha^{-1}(Y)$. Wir wollen diese Schreibweisen nicht verwenden, da dabei erst aus dem Zusammenhang oder aus der Art des Argumentes klar wird, ob eine Abbildung von A nach B oder eine solche von P(A) nach P(B) vorliegt. Außerdem ist im Falle einer bijektiven Abbildung α die Schreibweise α^{-1} schon für die inverse Abbildung von α reserviert.

Die induzierten Abbildungen α_p und α^p haben interessante Eigenschaften, auf die wir später im VI. Kapitel zurückkommen. Hier geben wir einige einfache Eigenschaften an.

Seien $\alpha : A \longrightarrow B$ und $\beta : B \longrightarrow C$ zwei Abbildungen. Dann gilt:

$$(\beta\alpha)_p = \beta_p\alpha_p \quad \text{und} \quad (\beta\alpha)^p = \alpha^p\beta^p \ .$$

Sei zunächst $X \in P(A)$, dann folgt

$$\begin{aligned}(\beta\alpha)_p(X) &= \{\beta\alpha(x) \mid x \in X\} = \{\beta(\alpha(x)) \mid x \in X\} \\ &= \beta_p(\{\alpha(x) \mid x \in X\}) = \beta_p(\alpha_p(X)) = \beta_p\alpha_p(X) \ .\end{aligned}$$

Für $Z \in P(C)$ gilt einerseits

$$(\beta\alpha)^p(Z) = \{a \mid a \in A \wedge \beta\alpha(a) \in Z\}$$

und andererseits

$$\begin{aligned}\alpha^p\beta^p(Z) &= \alpha^p(\{b \mid b \in B \wedge \beta(b) \in Z\}) \\ &= \{a \mid a \in A \wedge \beta(\alpha(a)) \in Z\}\end{aligned}$$

und wegen $\beta\alpha(a) = \beta(\alpha(a))$ gilt auch jetzt die Gleichheit.

Wie man sofort sieht, gilt auch

$$(1_A)_p = 1_{P(A)} \quad , \quad (1_A)^p = 1_{P(A)} \ .$$

Von Interesse ist weiterhin das Verhalten der induzierten Abbildungen im Bezug auf die Inklusion und die Operationen Vereinigung und Durchschnitt.

1.9.1 SATZ:
Sei $\alpha : A \longrightarrow B$ eine Abbildung und seien $X_1, X_2 \in P(A)$ sowie $Y_1, Y_2 \in P(B)$. Dann gilt:

1) $X_1 \subset X_2 \Longrightarrow \alpha_p(X_1) \subset \alpha_p(X_2)$,
2) $Y_1 \subset Y_2 \Longrightarrow \alpha^p(Y_1) \subset \alpha^p(Y_2)$,
3) $\alpha_p(X_1 \cap X_2) \subset \alpha_p(X_1) \cap \alpha_p(X_2)$,
4) $\alpha_p(X_1 \cup X_2) = \alpha_p(X_1) \cup \alpha_p(X_2)$,
5) $\alpha^p(Y_1 \cap Y_2) = \alpha^p(Y_1) \cap \alpha^p(Y_2)$,
6) $\alpha^p(Y_1 \cup Y_2) = \alpha^p(Y_1) \cup \alpha^p(Y_2)$.

Beweis:

1): $\alpha_p(X_1) = \{\alpha(x) \mid x \in X_1\} \subset \{\alpha(x) \mid x \in X_2\} = \alpha_p(X_2)$.

2): $x \in \alpha^p(Y_1) \Rightarrow \alpha(x) \in Y_1 \subset Y_2 \Rightarrow x \in \alpha^p(Y_2)$.

3): Folgt aus 1) , da $X_1 \cap X_2 \subset X_1$ und $X_1 \cap X_2 \subset X_2$.

4): Die Inklusion "$\supset$" folgt wieder aus 1) ; bleibt "$\subset$" zu zeigen. Sei $y \in \alpha_p(X_1 \cup X_2)$, dann gibt es ein $x \in X_1 \cup X_2$ mit $\alpha(x) = y$. Für $x \in X_1$ bzw. $x \in X_2$ folgt $y \in \alpha_p(X_1)$ bzw. $y \in \alpha_p(X_2)$, also $y \in \alpha_p(X_1) \cup \alpha_p(X_2)$.

5): "$\subset$" folgt aus 2) . Sei $x \in \alpha^p(Y_1) \cap \alpha^p(Y_2)$, dann folgt $\alpha(x) \in Y_1$ und $\alpha(x) \in Y_2$, also $\alpha(x) \in Y_1 \cap Y_2$ und folglich $x \in \alpha^p(Y_1 \cap Y_2)$.

6): "$\supset$" folgt aus 2). Sei $x \in \alpha^p(Y_1 \cup Y_2)$, dann folgt $\alpha(x) \in Y_1 \cup Y_2$, also $\alpha(x) \in Y_1$ oder $\alpha(x) \in Y_2$ und folglich $x \in \alpha^p(Y_1)$ oder $x \in \alpha^p(Y_2)$, woraus sich $x \in \alpha^p(Y_1) \cup \alpha^p(Y_2)$ ergibt.//

Man wird sich fragen, ob in der Behauptung 3) des Satzes nicht auch das Gleichheitszeichen gilt. Ein einfaches Beispiel zeigt, daß dies nicht der Fall ist. Seien $A = \{1,2\}$, $B = \{0\}$ und $\alpha : A \longrightarrow B$ definiert durch $\alpha(1) = \alpha(2) = 0$. Setze $X_1 = \{1\}$, $X_2 = \{2\}$, dann ist $X_1 \cap X_2 = \emptyset$, also $\alpha_p(X_1 \cap X_2) = \alpha_p(\emptyset) = \emptyset$. Andererseits ist $\alpha_p(X_1) = \alpha_p(X_2) = B$, also $\alpha_p(X_1) \cap \alpha_p(X_2) = B \neq \emptyset$.

1.9.2 SATZ:
Sei $\alpha : A \longrightarrow B$ eine Abbildung und seien $X \subset A$, $Y \subset B$. Dann gilt:

1) $X \subset \alpha^p \alpha_p(X)$,

2) $\alpha_p \alpha^p(Y) \subset Y$.

Beweis:
1): Sei $x \in X$. Dann ist $\alpha(x) \in \alpha_p(X)$, also $x \in \alpha^p \alpha_p(X)$.

2): Sei $u \in \alpha_p \alpha^p(Y)$. Dann gibt es ein $v \in \alpha^p(Y)$ mit $\alpha(v) = u$. Wegen $v \in \alpha^p(Y)$ gilt aber $\alpha(v) \in Y$, so daß $u \in Y$ folgt.//

§ 2 Äquivalenzrelationen

2.1 Definition, Äquivalenzklassen

2.1.1 DEFINITION:
Eine Äquivalenzrelation einer Menge A ist eine Relation $\varrho = (A,A,U)$, die folgende Eigenschaften hat:

(1) Reflexivität:
$\forall a \in A\,[(a,a) \in U]$

(2) Transitivität:
$\forall a,b,c \in A\,[(a,b) \in U \wedge (b,c) \in U \Rightarrow (a,c) \in U]$

(3) Symmetrie:
$\forall a,b \in A\,[(a,b) \in U \Rightarrow (b,a) \in U]$

Wie üblich führen wir das Symbol $\sim$ ein. Für $a,b \in A$ setze

$$a \sim b :\Leftrightarrow (a,b) \in U \quad ,$$

in Worten "a äquivalent b". Damit nehmen (1),(2),(3) aus der Definition die folgende Form an:

(1) $\forall a \in A\,[a \sim a]$

(2) $\forall a,b,c \in A\,[a \sim b \wedge b \sim c \Rightarrow a \sim c]$

(3) $\forall a,b \in A\,[a \sim b \Rightarrow b \sim a]$.

Für die Äquivalenzrelation $\varrho = (A,A,U)$ wird dann auch $(A,\sim)$ oder, falls keine Verwechslung möglich ist, auch nur $\sim$ geschrieben.

Wir geben jetzt einige Beispiele für Äquivalenzrelationen an.

1) Die identische Relation $1_A = (A,A,\{(a,a) \mid a \in A\})$, die, wie schon festgestellt, eine Abbildung ist, ist auch eine Äquivalenzrelation. Für sie gilt

$$a \sim b \Leftrightarrow a = b \quad ,$$

das heißt, die Gleichheit von Elementen in A ist eine Äquivalenzrelation. Unter Beachtung von (1) "stehen hier so wenig wie möglich Elemente miteinander in Relation". Das bedeutet auch, daß der Graph von 1_A als Teilmenge im Graphen

einer jeden anderen Äquivalenzrelation von A enthalten ist.

2) Die Relation $(A,A,A\times A)$ ist offensichtlich auch eine Äquivalenzrelation, deren Graph im Gegensatz zu dem von 1_A die Graphen aller Äquivalenzrelationen von A enthält.

3) Zu jeder Abbildung $\alpha : A \longrightarrow B$ gehört eine Äquivalenzrelation von A : Sei für $a_1, a_2 \in A$

$$a_1 \sim a_2 :\Longleftrightarrow \alpha(a_1) = \alpha(a_2) \quad ,$$

dann ist sofort zu bestätigen, daß (1),(2) und (3) erfüllt sind. Offensichtlich ist dies genau dann die identische Relation von A, wenn α injektiv ist.

4) Äquivalenzrelationen in der Menge $\mathbb{Z}$ der ganzen Zahlen erhält man auf folgende Weise: Sei $n \in \mathbb{Z}$, $n \neq 0$, dann wird für $a,b \in \mathbb{Z}$

$$a \sim b :\Longleftrightarrow n/a-b$$

definiert. Dabei bedeutet $n/a-b$, daß n Teiler von a-b ist, das heißt, daß ein $q \in \mathbb{Z}$ mit $a-b = qn$ existiert. Statt $a \sim b$ schreibt man jetzt meist

$$a \equiv b \pmod{n} \quad ,$$

in Worten: a ist kongruent b modulo n . Wir weisen noch darauf hin, daß $a \equiv b \pmod{n}$, also $n/a-b$ genau dann gilt, wenn a und b bei Division durch n mit Rest den gleichen Rest besitzen. Ist $a = qn + r$ mit $r \in \mathbb{Z}$, $0 \leq r < |n|$, dann ist r der eben genannte Rest.

2.1.2 DEFINITION:
Sei $(A,\sim)$ eine Äquivalenzrelation.

1) Für $a \in A$ heißt

$$\overline{a} := \{ x \mid x \in A \wedge x \sim a \}$$

die durch a erzeugte Äquivalenzklasse zur Äquivalenzrelation $(A,\sim)$.

2) Die Menge der Äquivalenzklassen zur Äquivalenzrelation $(A,\sim)$ wird mit $\overline{A} = A/\sim$ bezeichnet, also

$$\overline{A} = A/\sim \; := \{ \overline{a} \mid a \in A \} \; .$$

3) Gilt $b \in \bar{a}$, dann heißt b ein R e p r ä s e n t a n t der Äquivalenzklasse $\bar{a}$.

2.1.3 HILFSSATZ:
Sei $(A, \sim)$ eine Äquivalenzrelation, dann gilt:

1) $\quad b \in \bar{a} \iff \bar{a} = \bar{b}$,

das heißt, genau die Repräsentanten einer Äquivalenzklasse erzeugen die Äquivalenzklasse.

2) $\quad \forall a,b \in A \left[\bar{a} \neq \bar{b} \implies \bar{a} \cap \bar{b} = \emptyset \right]$,

das heißt, je zwei verschiedene Äquivalenzklassen sind disjunkt.

3) $\quad \bigcup_{a \in A} \bar{a} = A$,

das heißt, die Vereinigungsmenge aller Äquivalenzklassen von $(A, \sim)$ ist A .

Beweis:

1): Nach Definition der Äquivalenzklassen und der definierenden Eigenschaften (1),(2) und (3) einer Äquivalenzrelation, bestätigt man leicht:

$$b \in \bar{a} \iff b \sim a \iff \forall x \in A \left[x \sim b \iff x \sim a \right] \iff \bar{b} = \bar{a} .$$

2): Sei $\bar{a} \cap \bar{b} \neq \emptyset$ und sei $c \in \bar{a} \cap \bar{b}$, dann folgt nach 1) $\bar{c} = \bar{a}$ und $\bar{c} = \bar{b}$, also $\bar{a} = \bar{b}$.

3): Wegen $a \in \bar{a}$ folgt die Behauptung. //

2.2 Partitionen

Äquivalenzrelationen und Partitionen hängen eng miteinander zusammen, wie jetzt gezeigt werden soll.

2.2.1 DEFINITION:
Eine P a r t i t i o n $\mathfrak{P}$ einer Menge A ist eine Menge von nichtleeren, paarweise disjunkten Teilmengen von A , deren Vereinigung gleich A ist. In Zeichen:

$$\mathfrak{P} \subset P(A) \setminus \{\emptyset\} \wedge \forall X,Y \in \mathfrak{P} \; [X \neq Y \implies X \cap Y = \emptyset]$$
$$\wedge \bigcup_{X \in \mathfrak{P}} X = A .$$

Wie Hilfssatz 2.1.3 zeigt, ist zu einer beliebigen Äquivalenzrelation $(A,\sim)$ die Menge der Äquivalenzklassen

$$A/\sim \;=\; \{\,\bar{a} \mid a \in A\,\}$$

eine Partition von A .

Bemerkenswert ist nun, daß umgekehrt zu jeder Partition von A eine Äquivalenzrelation $(A,\sim)$ gehört, für die

$$\mathfrak{P} = A/\sim$$

gilt. Man definiert dazu für $a,b \in A$

$$a \sim b \;:\Longleftrightarrow\; \exists X \in \mathfrak{P}\; [a \in X \wedge b \in X] \quad ,$$

das heißt, es seien genau dann zwei Elemente äquivalent, wenn sie beide in einer der Mengen aus $\mathfrak{P}$ liegen. Wir prüfen die Bedingungen für eine Äquivalenzrelation nach.

Reflexivität: Da die Vereinigungsmenge aller $X \in \mathfrak{P}$ ganz A ist, liegt jedes $a \in A$ in mindestens einem $X \in \mathfrak{P}$, also gilt $a \sim a$.
Transitivität: Seien $a \sim b$, das heißt $a,b \in X \in \mathfrak{P}$ und $b \sim c$, das heißt $b,c \in Y \in \mathfrak{P}$. Es folgt $b \in X \cap Y$; wegen der Disjunktheit muß dann $X = Y$ gelten. Daraus folgt nach Definition der Äquivalenz $a \sim c$.
Symmetrie: $a \sim b$, das heißt $a,b \in X \in \mathfrak{P}$ und folglich gilt auch $b \sim a$.
Nach Definition von $A/\sim$ gilt dann offensichtlich $\mathfrak{P} = A/\sim$.

Ein wichtiges Beispiel für Partitionen ist die, die aus der Äquivalenzrelation in Beispiel 4) aus dem vorhergehenden Abschnitt entsteht. Dabei ist

$$\bar{a} = \{\,b \mid b \in \mathbb{Z} \wedge \exists q \in \mathbb{Z}\; [b = a + qn]\,\} \;=\; a + \mathbb{Z}n \quad .$$

Diese Partition wird mit $\mathbb{Z}/\,\mathbb{Z}n$ bezeichnet. Es gilt

$$\mathbb{Z}/\,\mathbb{Z}n = \{\,\bar{0}\,,\,\bar{1}\,,\,\ldots\,,\,\overline{n-1}\,\} \quad ,$$

denn wegen der Division mit Rest (siehe VII.2.2.6) ist jede Zahl in $\mathbb{Z}$ zu einer der Zahlen $0,1,\ldots,n-1$ äquivalent, was jetzt "kongruent modulo n" bedeutet. Wegen der Eindeutigkeit der Division mit Rest sind ferner je zwei der Zahlen aus $\{0,\ldots,n-1\}$ nicht äquivalent.

2.3 Faktorisierung

In Beispiel 3) aus 2.1 wurde festgestellt, daß zu jeder Abbildung $\alpha : A \longrightarrow B$ eine Äquivalenzrelation gehört, die durch

$$a \sim b \quad :\Longleftrightarrow \quad \alpha(a) = \alpha(b)$$

definiert wird. Wir wollen jetztüberlegen, daß man α über $A/\sim$ "faktorisieren" kann.

Dazu betrachten wir, wenn zunächst $(A,\sim)$ eine beliebige Äquivalenzrelation ist, die surjektive Abbildung

$$\nu : A \ni a \longrightarrow \bar{a} \in \bar{A} := A/\sim \quad ,$$

die also jedes Element $a \in A$ auf die durch a erzeugte Äquivalenzklasse

$$\bar{a} = \{ x \mid x \in A \wedge x \sim a \}$$

abbildet. Man nennt ν die zu $(A,\sim)$ gehörende n a t ü r l i c h e oder k a n o n i s c h e Surjektion.

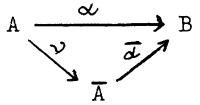
Sei jetzt wieder $(A,\sim)$ die zu $\alpha : A \longrightarrow B$ gehörende Äquivalenzrelation mit der Menge der Äquivalenzklassen $\bar{A} = A/\sim$. Dann kann eine injektive Abbildung

$$\bar{\alpha} : \bar{A} \longrightarrow B$$

so definiert werden, daß gilt

$$\alpha = \bar{\alpha}\,\nu \quad .$$

Man hat damit α als Produkt der Injektion $\bar{\alpha}$ und der Surjektion ν dargestellt. Das Bestehen der Gleichung $\alpha = \bar{\alpha}\,\nu$ drückt man auch dadurch aus, daß man sagt, das Diagramm



ist kommutativ.

Wir definieren nun $\bar{\alpha}$ durch die Festsetzung

$$\bar{\alpha} : \bar{A} \ni \bar{a} \longmapsto \alpha(a) \in B \quad .$$

Um zu sehen, daß dies tatsächlich eine Abbildung ist, muß festgestellt werden, daß es zu $\bar{a}$ nur ein Paar $(\bar{a}, \alpha(a))$ in

in $Gr(\alpha)$ gibt, das heißt, daß $\alpha(a)$ nicht von der Wahl des Repräsentanten a von $\bar{a}$ abhängt. Sei $\bar{a} = \bar{b}$, dann folgt $a \sim b$, und dies ist nach Definition von $\sim$ mit $\alpha(a) = \alpha(b)$ äquivalent. Also ist $\bar{\alpha}$ tatsächlich eine Abbildung. Sei nun $a \in A$, dann gilt

$$\bar{\alpha}\nu(a) = \bar{\alpha}(\nu(a)) = \bar{\alpha}(\bar{a}) = \alpha(a) ,$$

also $\bar{\alpha}\nu = \alpha$. Ist $\bar{\alpha}(\bar{a}) = \bar{\alpha}(\bar{b})$, so ist $\alpha(a) = \alpha(b)$, also $\bar{a} = \bar{b}$. Folglich ist $\bar{\alpha}$ injektiv.

Der soeben geschilderte Sachverhalt kann noch verallgemeinert werden, indem an Stelle der zu α gehörenden Äquivalenzrelation mit

$$a \sim b \iff \alpha(a) = \alpha(b)$$

eine beliebige "kleinere" (im Sinne der Inklusion der Graphen) Äquivalenzrelation tritt.

2.3.1 SATZ:
Sei $\alpha : A \longrightarrow B$ eine Abbildung und sei $\sim$ eine Äquivalenzrelation von A mit der Eigenschaft

$$\forall a,b \in A \left[a \sim b \implies \alpha(a) = \alpha(b) \right] .$$

Dann sind

$$\nu : A \ni a \longmapsto \bar{a} \in A/\sim$$

und

$$\bar{\alpha} : A/\sim \ni \bar{a} \longmapsto \alpha(a) \in B$$

Abbildungen mit

$$\alpha = \bar{\alpha}\nu$$

und $\bar{\alpha}$ ist durch die Gleichung $\alpha = \bar{\alpha}\nu$ eindeutig bestimmt.

Beweis: Der Beweis des vorhergehenden Spezialfalles (nämlich $a \sim b \iff \alpha(a) = \alpha(b)$) kann wörtlich übernommen werden. Es bleibt nur noch zu zeigen, daß $\bar{\alpha}$ durch $\alpha = \bar{\alpha}\nu$ eindeutig bestimmt ist. Sei dazu auch $\alpha = \beta\nu$ mit einer Abbildung

$$\beta : A/\sim \longrightarrow B ,$$

dann folgt

$$\bar{\alpha}(\bar{a}) = \alpha(a) = \beta\nu(a) = \beta(\bar{a}) \quad ,$$

also $\bar{\alpha} = \beta$ .//

Der Leser betrachte zur Übung den Fall, daß $\sim$ die identische Äquivalenzrelation ist.

Der vorstehende Satz kann auf endlich viele Äquivalenzrelationen ausgedehnt werden

2.3.2 SATZ:
Sei

$$\alpha : A_1 \times A_2 \times \ldots \times A_n \longrightarrow B$$

eine Abbildung und seien

$$(A_i, \sim_i) \quad , \quad i = 1,2,\ldots,n$$

Äquivalenzrelationen mit der Eigenschaft, daß für alle

$$(a_1,\ldots,a_n),(b_1,\ldots,b_n) \in A_1 \times \ldots \times A_n$$

mit

$$a_i \sim_i b_i \quad \text{für} \quad i = 1,\ldots,n$$

gilt

$$\alpha(a_1,\ldots,a_n) = \alpha(b_1,\ldots,b_n) \quad .$$

Dann sind

$$\mu : A_1 \times \ldots \times A_n \longrightarrow (A_1/\sim_1) \times \ldots \times (A_n/\sim_n)$$

mit

$$\mu(a_1,\ldots,a_n) := (\bar{a}_1,\ldots,\bar{a}_n)$$

und

$$\hat{\alpha} : (A_1/\sim_1) \times \ldots \times (A_n/\sim_n) \longrightarrow B$$

mit

$$\hat{\alpha}(\bar{a}_1,\ldots,\bar{a}_n) := \alpha(a_1,\ldots,a_n)$$

Abbildungen mit

$$\alpha = \hat{\alpha}/\mu$$

und $\hat{\alpha}$ ist durch die vorhergehende Gleichung eindeutig bestimmt.

Beweis:Wie im Beweis von 2.3.1 sind die Behauptungen leicht zu bestätigen. Die "Verträglichkeitsvoraussetzung"

$$a_i \sim_i b_i \ , \ i = 1,\ldots,n \Longrightarrow \alpha(a_1,\ldots,a_n) = \alpha(b_1,\ldots,b_n)$$

impliziert jetzt, daß $\hat{\alpha}$ eine Abbildung ist.//

§ 3 Ordnungen

3.1 Definitionen und Bezeichnungen

3.1.1 DEFINITION:
Eine O r d n u n g (oder Anordnung) einer Menge A ist eine Relation $\varsigma = (A,A,U)$, die folgende Eigenschaften erfüllt:

(1) R e f l e x i v i t ä t :
$\forall a \in A\,[(a,a) \in U]$

(2) T r a n s i t i v i t ä t :
$\forall a,b,c \in A\,[(a,b) \in U \wedge (b,c) \in U \Rightarrow (a,c) \in U]$

(3) A n t i s y m m e t r i e :
$\forall a,b \in A\,[(a,b) \in U \wedge (b,a) \in U \Rightarrow a = b]$

Wir führen nun die übliche Bezeichnungsweise ein. Für $a,b \in A$ setze man :

$$a \leq b :\Leftrightarrow (a,b) \in U \quad ,$$
$$a < b :\Leftrightarrow a \leq b \wedge a \neq b \quad ,$$
$$a \not< b :\Leftrightarrow (a,b) \notin U \quad .$$

In dieser Schreibweise nehmen die Bedingungen (1),(2),(3) aus der Definition die folgende Form an:

(1) $\forall a \in A\,[a \leq a]$,
(2) $\forall a,b,c \in A\,[a \leq b \wedge b \leq c \Rightarrow a \leq c]$,
(3) $\forall a,b \in A\,[a \leq b \wedge b \leq a \Rightarrow a = b]$.

Für die Ordnung $\varsigma = (A,A,U)$ schreibt man auch $\varsigma = (A, \leq)$ oder nur kurz $\leq$, und man nennt A eine g e o r d n e t e Menge mit der Ordnung $\leq$.

Ist $\varsigma = (A,A,U)$ eine Ordnung von A und ist B eine Teilmenge von A, dann ist die Einschränkung der Ordnung ς auf B ,

$$\varsigma|B := (B,B,U \cap (B \times B)) \ ,$$

offensichtlich eine Ordnung von B. Sprechen wir von Teilmengen einer geordneten Menge, dann verstehen wir darunter stets geordnete Teilmengen in diesem Sinne.

Wie unmittelbar klar ist, ist die Gleichheitsrelation in einer Menge A eine Ordnung von A , für die gilt:

$$a \leq b \iff a = b \quad .$$

Betrachtet man eine solche Ordnung als trivial, so kann man Ordnungen, wie wir sie jetzt definieren, als das "Gegenteil" der trivialen Ordnung ansehen.

3.2 Totale Ordnungen

3.2.1 DEFINITION:
Eine Ordnung $\leq$ von A heißt t o t a l e O r d n u n g von A : $\iff \forall a,b \in A \,[a \leq b \vee b \leq a]$
Ist $\leq$ eine totale Ordnung von A , dann heißt A (bei $\leq$) t o t a l g e o r d n e t e M e n g e oder K e t t e .

Offenbar sind Teilmengen von total geordneten Mengen wieder total geordnet. Die übliche Ordnung der reellen Zahlen ist eine totale Ordnung.

Um ein nichttriviales Beispiel für eine Ordnung zu erhalten, die keine totale Ordnung ist, betrachten wir zu einer Menge A die Potenzmenge P(A) . Diese ist mit der Inklusion $\subset$ von Teilmengen von A als Ordnungsrelation eine geordnete Menge:

(1) $\forall X \in P(A) \,[X \subset X]$
(2) $\forall X,Y,Z \in P(A) \,[X \subset Y \wedge Y \subset Z \Rightarrow X \subset Z]$
(3) $\forall X,Y \in P(A) \,[X \subset Y \wedge Y \subset X \Rightarrow X = Y]$

Wie leicht zu sehen, ist P(A) mit dieser Ornung dann und nur dann total geordnet, wenn $A = \emptyset$ oder A genau ein Element besitzt. Besitzt also A mindestens zwei Elemente, so ist P(A) nicht total geordnet. Sind etwa $a,b \in A$, $a \neq b$, so gilt $\{a\} \not\subseteq \{b\}$ und $\{b\} \not\subseteq \{a\}$.

Später werden wir von der folgenden Eigenschaft einer total geordneten Menge Gebrauch machen.

3.2.2 HILFSSATZ:
Ist A eine total geordnete Menge mit der Ordnung $\leq$, dann können je endlich viele Elemente aus A stets so numeriert

werden, daß gilt:

$$a_1 \leq a_2 \leq \ldots \leq a_n \quad .$$

Beweis: Durch Induktion nach n , wobei der Induktionsbeginn n = 1 klar ist. Seien jetzt $a_1,\ldots,a_n$ gegeben und gelte schon nach Induktionsannahme

$$a_1 \leq a_2 \leq \ldots \leq a_{n-1} \quad .$$

Entweder ist $a_{n-1} \leq a_n$, dann ist man fertig, oder es gilt $a_n \leq a_{n-1}$. Dann können $a_1,\ldots,a_{n-2},a_n$ in der gewünschten Weise numeriert werden; seien dies etwa

$$b_1 \leq b_2 \leq \ldots \leq b_{n-1} \quad .$$

Für $b_n := a_{n-1}$ erhält man dann wie gewünscht

$$b_1 \leq b_2 \leq \ldots \leq b_n \quad .//$$

3.3 Supremum und Infimum

Wir betrachten jetzt wieder eine beliebige geordnete Menge.

3.3.1 DEFINITION:
Sei $(A, \leq)$ eine geordnete Menge.

(1) $a_0 \in A$ heißt ein m a x i m a l e s bzw. m i n i m a l e s Element in A : $\Leftrightarrow$

$\forall a \in A \,[a_0 \leq a \Rightarrow a_0 = a]$ bzw. $\forall a \in A \,[a \leq a_0 \Rightarrow a = a_0]$

(2) $a_0 \in A$ heißt g r ö ß t e s bzw. k l e i n s t e s Element in A : $\Leftrightarrow$

$\forall a \in A \,[a \leq a_0]$ bzw. $\forall a \in A \,[a_0 \leq a]$.

(3) $a_0 \in A$ heißt eine o b e r e bzw. u n t e r e S c h r a n k e einer Teilmenge B aus A : $\Leftrightarrow$

$\forall b \in B \,[b \leq a_0]$ bzw. $\forall b \in B \,[a_0 \leq b]$.

(4) Sei $B \subset A$. Besitzt die Menge der oberen Schranken von B in A ein kleinstes Element, so heißt dieses S u p r e m u m von B in A , in Zeichen sup(B). Besitzt die Menge der unteren Schranken von B in A ein größtes Element, so heißt dieses I n f i m u m von B in A , in Zeichen inf(B) .

Eine geordnete Menge braucht weder ein größtes noch ein kleinstes, weder ein maximales noch ein minimales Element zu besitzen, wie die Menge der reellen Zahlen zeigt. Sie kann auch mehrere maximale oder minimale Elemente besitzen. Zum Beispiel ist bei der Gleichheitsrelation einer Menge als Ordnung jedes Element maximales und minimales Element und, falls die Menge mehr als ein Element besitzt, gibt es kein größtes und kein kleinstes Element. Falls in einer geordneten Menge ein größtes bzw. kleinstes Element existiert, ist dies, wie sofort aus der Definition folgt, eindeutig bestimmt.

3.4 Wohlordnung und transfinite Induktion

3.4.1 DEFINITION:
Eine Ordnung einer Menge A heißt eine W o h l o r d n u n g von A , wenn jede nichtleere Teilmenge von A ein kleinstes Element besitzt. Eine Menge A zusammen mit einer Wohlordnung heißt eine w o h l g e o r d n e t e M e n g e .

Es ist klar, daß eine Wohlordnung einer Menge A eine totale Ordnung ist; hat man nämlich zwei Elemente $a,b \in A$ so muß die Menge $\{a,b\}$ ein kleinstes Element besitzen, das heißt, es gilt entweder $a \leq b$ oder $b \leq a$.

Zum Beispiel ist die Menge $\mathbb{N}$ der natürlichen Zahlen bei der natürlichen Ornung wohlgeordnet. Hingegen ist $\mathbb{R}$ nicht wohlgeordnet.

Für wohlgeordnete Mengen gilt die transfinite Induktion, die, zusammen mit dem im Anschluß erläuterten Wohlordnungssatz, eines der wichtigsten Beweisprinzipien für unendliche Mengen darstellt. Um dies auszuführen, brauchen wir den schon in II.1.6 erwähnten Begriff des Abschnitts.

3.4.2 DEFINITION:
Sei $(A, \leq)$ eine wohlgeordnete Menge und sei $a \in A$. Die Menge

$$Ab(a) := \{x \mid x \in A \wedge x < a\}$$

heißt der A b s c h n i t t von a .

Man beachte dabei, daß für das kleinste Element $a_0 \in A$ $Ab(a) = \emptyset$ gilt.

3.4.3 SATZ VON DER TRANSFINITEN INDUKTION:
Sei $(A, \leq)$ eine wohlgeordnete Menge und sei $U \subset A$ mit der folgenden Eigenschaft:

$$\forall a \in A \left[Ab(a) \subset U \implies a \in U \right] ,$$

dann gilt $U = A$.

Beweis: Indirekt. Angenommen $U \neq A$, dann folgt $A \setminus U \neq \emptyset$. Sei b ein kleinstes Element aus $A \setminus U$. Es folgt $Ab(b) \subset U$, denn jedes Element echt kleiner als b liegt in U. Nach Voraussetzung über U folgt $b \in U$ im Widerspruch zu $b \in A \setminus U$ .//

Es liegt auf der Hand, wie dieser Satz zum Beweis durch t r a n s f i n i t e I n d u k t i o n angewendet wird. Sei E(a) eine von $a \in A$ abhängende Aussage, die für $a \in A$ immer dann gilt, wenn sie für jedes $x \in Ab(a)$ gilt. Behauptung: Dann gilt E(a) für jedes $a \in A$. Um dies einzusehen, sei U in 3.4.3 die Erfüllungsmenge von E(a) , das heißt, die Menge der $a \in A$, für die E(a) gilt; 3.4.3 besagt dann $U = A$.

Man beachte, daß die transfinite Induktion, angewendet auf die Menge $\mathbb{N}$ der natürlichen Zahlen nur eine zur vollständigen Induktion (siehe VII.1) äquivalente Aussage liefert. Im allgemeinen Fall versagt jedoch die vollständige Induktion, da es Elemente gibt, die keinen "Vorgänger" besitzen; diese werden duch vollständige Induktion nicht "erreicht".

Im Hinblick auf die transfinite Induktion ist selbstverständlich die Frage von Interesse, welche Mengen eine Wohlordnung besitzen. Als eine Antwort auf diese Frage kann bewiesen werden, daß die folgenden Aussagen äquivalent sind:

(1) W o h l o r n u n g s s a t z : Jede Menge kann wohlgeordnet werden (d.h. besitzt mindestens eine Wohlordnung).

(2) Z o r n s c h e s L e m m a : Besitzt in einer wohlgeordneten Menge A jede total geordnete Teilmenge eine obere Schranke, so gibt es in A ein maximales Element.

(3) A u s w a h l a x i o m : Zu jeder Menge $M \neq \emptyset$ gibt es eine Abbildung

$$f : P(M) \longrightarrow M$$

mit $f(U) \in U$ für jedes $U \in P(M)$, $U \neq \emptyset$; das heißt, f "wählt" aus jeder nichtleeren Teilmenge U von M ein Element, nämlich f(U) aus.

Diese äquivalenten Aussagen, die wir als transfinite Hilfsmittel bezeichnen wollen, sind selbst nicht beweisbar. Welche man davon als Axiom und welche man entsprechend als Sätze betrachtet, ist vom logischen Standpunkt aus willkürlich. Historisch ist man vom Auswahlaxiom ausgegangen (E. Z e r m e l o 1904), was auch der Intuition entspricht.

Da hier die Äquivalenz von (1),(2),(3) nicht bewiesen werden soll und das Zornsche Lemma für unsere Zwecke am geeignetsten ist, soll dies hier als Axiom betrachtet und davon uneingeschränkt Gebrauch gemacht werden.

3.5 Verbände

Verbände kommen in vielen Gebieten der Mathematik vor. Wir wollen hier die wichtigsten Grundbegriffe über Verbände kennen lernen.

3.5.1 DEFINITION:

(1) Ein V e r b a n d ist eine geordnete Menge, in der jede zweielementige Teilmenge ein Supremum und ein Infimum besitzt.

(2) Ein Verband heißt v o l l s t ä n d i g , wenn jede Teilmenge ein Supremum und ein Infimum besitzt.

Durch Induktion ist leicht zu zeigen, daß in einem Verband jede nichtleere endliche Teilmenge ein Supremum und ein Infimum besitzt. Ein vollständiger Verband enthält offenbar ein größtes Element, nämlich das Supremum der ganzen Menge, das auch Infimum der leeren Teilmenge ist, und ein kleinstes Element, nämlich das Infimum der ganzen Menge, das auch Supremum der leeren Teilmenge ist.

Setzt man in einem Verband A für $a,b \in A$:

$$a \cup b := \sup\{a,b\} \ ,$$
$$a \cap b := \inf\{a,b\} \ ,$$

dann lassen sich die folgenden Begriffe, die Vertauschbarkeitsbedingungen für Suprema und Infima enthalten, kurz formulieren.

3.5.2 DEFINITION:

(1) Ein Verband $(A, \leq)$ heißt m o d u l a r $:\Longleftrightarrow$

$$\forall a,b,c \in A \left[a = a \cap c \Longrightarrow (a \cup b) \cap c = a \cup (b \cap c) \right] .$$

(2) Ein Verband $(A, \leq)$ heißt d i s t r i b u t i v $:\Longleftrightarrow$

$$\forall a,b,c \in A \left[(a \cup b) \cap c = (a \cap c) \cup (b \cap c) \right] .$$

Dabei ist bemerkenswert, daß die einen distributiven Verband definierende Bedingung

$$(a \cup b) \wedge c = (a \cap c) \cup (b \wedge c)$$

mit der Bedingung

$$(a \cap b) \cup c = (a \cup c) \wedge (b \cup c)$$

äquivalent ist.

Gewisse distributive Verbände spielen eine besonders wichtige Rolle, die sogenannten Booleschen Verbände.

3.5.3 DEFINITION:
Ein Verband $(A, \leq)$ heißt B o o l e s c h e r Verband $:\Longleftrightarrow$

(1) A ist distributiv,
(2) A enthält ein größtes Element e und ein kleinstes Element o,
(3) $\forall a \in A \ \exists a' \in A \left[a \cup a' = e \wedge a \cap a' = o \right]$.

Zu (3) zeigen wir noch, daß a' durch a und (3) eindeutig bestimmt ist. Sei auch

$$a \cup b = e \wedge a \cap b = o \ ,$$

dann folgt

$$(a \cup a') \cap b = e \cap b = b$$

und andererseits bei Benutzung des distributiven Gesetzes aus 3.5.2

$$(a \cup a') \cap b = (a \cap b) \cup (a' \cap b)$$
$$= o \cup (a' \cap b) = a' \cap b \quad ,$$

also $b = a' \cap b$, und dies bedeutet $b \leq a'$. Analog folgt auch $a' \leq b$, so daß $a' = b$ gilt.

Aus der Eindeutigkeit von a' folgt auch, daß

$$\varkappa : A \ni a \longmapsto a' \in A$$

eine Abbildung ist.

Ein Beispiel für einen Booleschen Verband ist die Potenzmenge $P(M)$ zu einer beliebigen Menge M mit der Inklusion als Ordnungsrelation. In diesem Falle ist $e = M$, $o = \emptyset$ und $A' = M \setminus A$ für $A \in P(M)$. Die Symbole $\cap$ und $\cup$ im Booleschen Verband stimmen jetzt mit Durchschnitt und Vereinigung überein.

Im nächsten Kapitel werden wir bei der Untersuchung der Booleschen Algebren auf die Booleschen Verbände zurückkommen.

Als Abschwächung des Verbandsbegriffes spielt der Begriff der filtrierten oder gefilterten Mengen eine wichtige Rolle für die Definition von Limites.

3.5.4 DEFINITION:
Eine geordnete Menge A heißt nach l i n k s oder u n t e n bzw. nach r e c h t s oder o b e n f i l t r i e r t : $\Longleftrightarrow$ jede zweielementige Teilmenge von A hat eine untere bzw. obere Schranke.

IV. Kapitel: Algebraische Strukturen

§ 1 Operationen und Monoide

1.1 Grundbegriffe und Beispiele

1.1.1 DEFINITION:
Sei G eine Menge. Eine (binäre) O p e r a t i o n oder V e r k n ü p f u n g in G ist eine Abbildung

$$\gamma : G \times G \longrightarrow G \quad .$$

Für das Bild $\gamma((a,b))$ von $(a,b) \in G \times G$ bei γ werden verschiedene Bezeichnungen verwendet, die von weiteren Eigenschaften von γ und dem Zusammenhang, in dem γ auftritt, abhängen. Zum Beispiel kommen für $\gamma((a,b))$ folgende Bezeichnungen vor:

$$a + b \ , \ a \cdot b \ , \ ab \ , \ a \circ b \ , \ a \cap b \ , \ a \cup b \quad .$$

Wir schreiben zunächst $\gamma(a,b) := \gamma((a,b))$ und wollen jetzt einige Bedingungen für γ formulieren.

1.1.2 DEFINITION:

(1) A s s o z i a t i v e s G e s e t z :
$\forall a,b,c \in G \left[\gamma(a,\gamma(b,c)) = \gamma(\gamma(a,b),c)\right]$

(2) Existenz eines n e u t r a l e n E l e m e n t e s :
$\exists e \in G \, \forall a \in G \left[\gamma(a,e) = \gamma(e,a) = a\right]$

(3) Existenz von i n v e r s e n E l e m e n t e n
(falls ein neutrales Element e existiert) :
$\forall a \in G \, \exists a' \in G \left[\gamma(a,a') = \gamma(a',a) = e\right]$

(4) K o m m u t a t i v e s G e s e t z :
$\forall a,b \in G \left[\gamma(a,b) = \gamma(b,a)\right]$.

Im Falle $ab := \gamma(a,b)$ bzw. $a + b := \gamma(a,b)$ nehmen diese Bedingungen die folgende Form an (,wobei wir die Quantoren weglassen):

(1)	$a(bc) = (ab)c$	$a + (b + c) = (a + b) + c$
(2)	$ae = ea = a$	$a + e = e + a = a$
(3)	$aa' = a'a = e$	$a + a' = a' + a = e$
(4)	$ab = ba$	$a + b = b + a$.

Gewisse Kombinationen dieser Bedingungen ergeben bekannte Operationen.

1.1.3 DEFINITION:
Eine Operation $\gamma : G \times G \longrightarrow G$ heißt

1) H a l b g r u p p e : $\Longleftrightarrow$ (1) gilt.
2) M o n o i d : $\Longleftrightarrow$ (1) $\wedge$ (2) gelten.
3) G r u p p e : $\Longleftrightarrow$ (1) $\wedge$ (2) $\wedge$ (3) gelten .
4) K o m m u t a t i v e oder a b e l s c h e
G r u p p e : $\Longleftrightarrow$ (1) $\wedge$ (2) $\wedge$ (3) $\wedge$ (4) gelten .

Beispiele für derartige Operationen sind schon im Bereich der Schulmathematik leicht anzugeben.

1) $\mathbb{N}$ ist mit der Addition als Operation eine Halbgruppe, aber kein Monoid.

2) $\mathbb{N}$ ist mit der Multiplikation als Operation ein Monoid mit dem neutralen Element 1 , aber keine Gruppe.

3) Die Menge aller Abbildungen einer Menge M nach M ist mit dem Produkt (= Hintereinanderausführung) von Abbildungen als Operation ein Monoid mit der identischen Abbildung als neutralem Element (ist $M = \emptyset$, so ist $(\emptyset,\emptyset,\emptyset)$ die identische Abbildung !).

4) $\mathbb{Z}$ ist mit der Addition als Operation eine Gruppe mit dem neutralen Element 0.

5) $\mathbb{R} \setminus \{0\}$ ist mit der Multiplikation als Operation eine Gruppe mit dem neutralen Element 1. Man beachte, daß $\mathbb{R}$ mit der Multiplikation als Operation keine Gruppe, sondern nur ein Monoid ist.

Das assoziative Gesetz besagt für eine multiplikativ geschriebene Halbgruppe, daß es bei einem Produkt von drei Faktoren nicht auf die Reihenfolge der Produktbildung

ankommt, so daß man Klammern weglassen kann. Diese Eigenschaft überträgt sich induktiv auf Produkte von mehr als drei Faktoren.

Für die Elemente einer multiplikativ geschriebenen Halbgruppe G benutzen wir die übliche Potenzschreibweise. Sei $a \in G$, $n \in \mathbb{N}$, dann sei

$$a^n := \underbrace{aa \ldots a}_{n \text{ Faktoren}} .$$

Für $m,n \in \mathbb{N}$ gilt dann

$$a^m a^n = a^{m+n} .$$

Ist G sogar ein Monoid, dann setze man $a^0 := e$.

In additiver Schreibweise hat man entsprechend, wenn das neutrale Element des Monoids G mit 0 bezeichnet wird:

$$na := \underbrace{a+a+\ldots+a}_{n \text{ Summanden}} , \qquad 0a := 0 .$$

Man beachte dabei, daß in $0a = 0$ die erste 0 in $\mathbb{Z}$ und die zweite 0 in G liegt.

Schließlich definieren wir noch strukturerhaltende Abbildungen.

1.1.4 DEFINITION:

(1) Seien (G, γ) und (H, η) zwei Halbgruppen. Eine Abbildung $\varphi : G \longrightarrow H$ heißt (H a l b g r u p p e n -) H o m o m o r p h i s m u s $:\Longleftrightarrow$

$$\forall a,b \in G \quad \varphi(\gamma(a,b)) = \eta(\varphi(a),\varphi(b)) .$$

(2) Seien (G, γ) und (H, η) zwei Monoide mit den neutralen Elementen e bzw. e'. Eine Abbildung $\varphi : G \longrightarrow H$ heißt (M o n o i d -) H o m o m o r p h i s m u s $:\Longleftrightarrow$ φ ist ein Halbgruppenhomomorphismus und es gilt $\varphi(e) = e'$.

Entsprechend werden Homomorphismen für Gruppen und andere algebraische Strukturen definiert, auf die wir später zurückkommen.

1.2 Monoide

Es sollen jetzt einige Eigenschaften für ein Monoid bewiesen werden, die wir später in verschiedenen Fällen brauchen. Dazu wird die Operation des Monoids G in der Form ab geschrieben, also als Multiplikation; dennoch werden die Resultate später auch für Monoide mit additiv geschriebener Operation benutzt.

Sei also G im folgenden ein Monoid.

1.2.1 BEHAUPTUNG:
Das neutrale Element eines Monoids ist eindeutig bestimmt.

Beweis: Seien e und e' neutrale Elemente von G , dann folgt

$$e' = ee' = e \ .$$

Hierbei wird nur benutzt, daß e "Linksidentität" von e' und e' "Rechtsidentität" von e ist.//

1.2.2 DEFINITION:
Seien $a,b,c,d \in G$. Dann heißt b R e c h t s i n v e r s e s bzw. c L i n k s i n v e r s e s bzw. d I n v e r s e s von a :$\Leftrightarrow$

$$ab = e \quad \text{bzw.} \quad ca = e \quad \text{bzw.} \quad ad = da = e \ .$$

Existiert ein Rechtsinverses bzw. ein Linksinverses bzw. ein Inverses von a , dann heißt a r e c h t s i n v e r t i e r b a r oder R e c h t s e i n h e i t bzw. l i n k s i n v e r t i e r b a r oder L i n k s e i n h e i t bzw. i n v e r t i e r b a r oder E i n h e i t .

1.2.3 BEHAUPTUNG:
Aus $ab = e$ und $ca = e$ folgt $b = c$. Folglich ist dann $b = c$ ein Inverses von a , und falls a ein Inverses besitzt, so ist dieses eindeutig bestimmt.

Beweis: $b = eb = (ca)b = c(ab) = ce = c$ .//

Wird die Operation des Monoids G multiplikativ geschrieben, und ist $a \in G$ invertierbar, dann wird das Inverse von a

mit a^{-1} bezeichnet. Wird die Operation von G als Addition geschrieben, dann bezeichne -a das Inverse von a und es wird $b - a := b + (-a)$ gesetzt.

1.2.4 BEHAUPTUNG:
Ist a invertierbar, dann auch a^{-1} , und es gilt $(a^{-1})^{-1} = a$.
Sind a und b invertierbar, dann auch ab , und es gilt $(ab)^{-1} = b^{-1}a^{-1}$.

Beweis: Wegen $aa^{-1} = a^{-1}a = e$ ist a^{-1} invertierbar und es gilt $(a^{-1})^{-1} = a$, da das Inverse eindeutig bestimmt ist und a ein Inverses von a^{-1} ist. Wegen

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e \quad ,$$
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

ist ab invertierbar mit dem Inversen $b^{-1}a^{-1}$, also gilt $(ab)^{-1} = b^{-1}a^{-1}$ .//

Ist a^{-1} das Inverse von a , dann wird für $n \in \mathbb{N}$

$$a^{-n} := (a^{-1})^n$$

gesetzt. Wie man durch Induktion über n leicht zeigt, gilt dann $a^{-n} = (a^n)^{-1}$, also $(a^{-1})^n = (a^n)^{-1}$.

Eine Konstruktion, die im Falle von Monoiden und Gruppen besonders wichtig ist, liefert weitere Beispiele für solche Operationen. Sei (G,γ) eine Menge mit einer Operation γ und sei $A \neq \emptyset$ eine Menge. Dann wird in der Menge G^A aller Abbildungen von A nach G eine Operation

$$\hat{\gamma} : G^A \times G^A \longrightarrow G^A$$

durch

$$\forall f,g \in G^A \, \forall a \in A \left[\hat{\gamma}(f,g)(a) := \gamma(f(a),g(a)) \right]$$

definiert. Ist (G,γ) eine Halbgruppe bzw. ein Monoid bzw. eine Gruppe, so ist $(G^A,\hat{\gamma})$ eine gleiche Operation. Ist etwa (G,γ) ein Monoid mit dem neutralen Element e , so ist

$$h : A \longrightarrow G \quad \text{mit} \quad h(a) := e \quad \text{für alle } a \in A$$

ein neutrales Element von $(G^A,\hat{\gamma})$. Der Leser möge zur Übung weitere Eigenschaften nachprüfen.

§ 2 Gruppen

2.1 Kennzeichnung von Gruppen

Es sollen jetzt Eigenschaften von Gruppen angegeben werden, wobei die Gruppenoperation als Multiplikation geschrieben wird. Sei also G eine multiplikative Gruppe mit dem neutralen Element e .

2.1.1 BEHAUPTUNG:

$$\forall a \in G \; [a^2 = a \Longleftrightarrow a = e]$$

Beweis:"$\Rightarrow$": $a^2 = a \Rightarrow e = aa^{-1} = a^2a^{-1} = a(aa^{-1}) = ae = a$.
"$\Leftarrow$": $e^2 = e$, da e das neutrale Element ist.//

2.1.2 SATZ:
Sei G eine Halbgruppe und $G \neq \emptyset$. Dann sind äquivalent:

(1) G ist eine Gruppe ,

(2) $\forall a \in G \; [a^{(\ell)} : G \ni x \longmapsto ax \in G$ ist bijektiv $\wedge$
$a^{(r)} : G \ni x \longmapsto xa \in G$ ist bijektiv$]$,

(3) $\forall a \in G \; [a^{(\ell)} : G \ni x \longmapsto ax \in G$ ist surjektiv $\wedge$
$a^{(r)} : G \ni x \longmapsto xa \in G$ ist surjektiv$]$.

Beweis:(1) $\Rightarrow$ (2): Die Umkehrabbildung zu $a^{(\ell)}$ ist $(a^{-1})^{(\ell)}$, die zu $a^{(r)}$ ist $(a^{-1})^{(r)}$. Nach III.1.6.1 folgt, daß $a^{(\ell)}$ und $a^{(r)}$ bijektiv sind.
(2) $\Rightarrow$ (3): Klar.
(3) $\Rightarrow$ (1): Existenz eines neutralen Elementes: Sei $a \in G$ $\Rightarrow \exists e \in G \; [ae = a]$, da $a^{(\ell)}$ surjektiv. Sei $b \in G \Rightarrow \exists c \in G$ $[ca = b]$, da $a^{(r)}$ surjektiv. Daraus folgt

$$be = cae = ca = b \quad ,$$

also gilt $be = b$ für alle $b \in G$. Analog erhält man ein $e' \in G$ mit $e'b = b$ für alle $b \in G$. Dann folgt $e' = e'e = e$, also ist e neutrales Element von G .
Existenz von inversen Elementen: Da $a^{(r)}$ und $a^{(\ell)}$ surjektiv sind, gibt es $b,c \in G$ mit $ba = e$ und $ac = e$. Dann folgt $b = be = bac = ec = c$, also ist $b = c$ Inverses von a .//

Die Aussagen (2) und (3) dieses Satzes lassen sich auch folgendermaßen ausdrücken: Jede Gleichung $ax = b$ und $ya = b$ hat eine (eindeutig bestimmte) Lösung.

Man kann bei einer endlichen Halbgruppe die Multiplikation $\mu: G \times G \longrightarrow G$ auch in Form einer sogenannten M u l t i p l i k a t i o n s t a f e l beschreiben:

	a_1	a_2	. . .	a_n
a_1	$\mu(a_1,a_1)$	$\mu(a_1,a_2)$	. . .	$\mu(a_1,a_n)$
a_2	$\mu(a_2,a_1)$	$\mu(a_2,a_2)$	. . .	$\mu(a_2,a_n)$
.	.	.		.
.	.	.		.
.	.	.		.
a_n	$\mu(a_n,a_1)$	$\mu(a_n,a_2)$	. . .	$\mu(a_n,a_n)$

Sei (G,μ) eine Halbgruppe mit $G \neq \emptyset$. Dies ist genau dann eine Gruppe, wenn in jeder Zeile und in jeder Spalte der Multiplikationstafel alle Elemente aus G (genau einmal) vorkommen.

Sei G eine Gruppe. Dann ist auch

$$\tau_a : G \ni x \longmapsto a^{-1}xa \in G$$

eine Bijektion, da $\tau_a = (a^{-1})^{(\ell)} a^{(r)}$ die Hintereinanderausführung von $a^{(r)}$ und $(a^{-1})^{(\ell)}$ ist. τ_a nennt man auch den durch a erzeugten i n n e r e n A u t o m o r p h i s m u s von G .

2.2 Die Gruppe der invertierbaren Elemente eines Monoids

2.2.1 BEHAUPTUNG:
Die invertierbaren Elemente in einem Monoid G bilden bei der Operation von G eine Gruppe mit dem gleichen neutralen Element wie G .

Beweis: Folgt aus 1.2.4.//

2.2.2 FOLGERUNG:
Die Bijektionen einer Menge M auf sich bilden bei der Hintereinanderausführung als Operation eine Gruppe.

Beweis: Folgt aus 2.2.1 und III.1.6.1.//

2.2.3 DEFINITION:
Ist M eine Menge mit n Elementen, dann heißen die Bijektionen von M auf sich P e r m u t a t i o n e n und die Gruppe aller Permutationen heißt die s y m m e t r i s c h e G r u p p e von n Elementen, in Zeichen S_n .

In die Bezeichnung S_n geht nicht ein, welche Menge M mit n Elementen man zugrunde legt, da dies unwesentlich ist (siehe dazu 2.8) . Als Menge M mit n Elementen wird meist die Menge $\{1,2,\ldots,n\}$ betrachtet. Für eine Permutation π dieser Menge wird auch die folgende Schreibweise benutzt:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix} := \pi \quad ,$$

das heißt, man schreibt in diesem Schema das Bild jeweils unter das Urbild. Die Zahlen $\pi(1), \pi(2), \ldots, \pi(n)$ sind dann genau wieder die Zahlen $1,2,\ldots,n$, nur in einer anderen Reihenfolge falls $\pi \neq 1_M$. Schreibt man umgekehrt

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

mit $\{a_1,\ldots,a_n\} = \{1,\ldots,n\}$,so wird dadurch eine Permutation definiert. Man erhält also genau alle Permutationen π von $\{1,\ldots,n\}$, wenn man unter die Zahlen $1,\ldots,n$ (in der natürlichen Ordnung hingeschrieben) dieselben Zahlen in allen möglichen Anordnungen darunter schreibt.

2.3 Untergruppen

Ist eine algebraische oder sonstige Struktur gegeben, dann sind "Unterstrukturen" von Interesse, das sind Teilmengen der Struktur, die bei "Einschränkung" der Struktur auf diese Teilmenge wieder eine solche (oder damit zusammenhängende) Struktur darstellen. Ein Beispiel hierfür stellen die Untergruppen einer Gruppe dar.

2.3.1 DEFINITION:
Sei G eine multiplikativ geschriebene Gruppe.

1) Eine Teilmenge H von G heißt U n t e r g r u p p e von G , wenn H bei der Einschränkung der Gruppenopertion von G auf H , daß heißt bei

$$H \times H \ni (h_1, h_2) \longmapsto h_1 h_2 \in H$$

eine Gruppe ist. Ist H Untergruppe von G , dann wird $H \leq G$ geschrieben.

2) Eine Untergruppe H von G heißt N o r m a l t e i l e r von G $:\Longleftrightarrow$

$$\forall a \in G \left[a^{-1}Ha := \{ a^{-1}ha \mid h \in H \} = H \right] .$$

Wir weisen zunächst darauf hin, das die Definition der Untergruppe die Forderung einschließt, daß für $h_1, h_2 \in H$ auch $h_1 h_2 \in H$ gilt. Sei $H \leq G$ und sei e' das neutrale Element von H , dann gilt $e'e' = e'$; nach 2.1.1 genügt aber nur das neutrale Element e von G dieser Gleichung, so daß $e' = e$ folgt. Dann folgt wegen der Eindeutigkeit des Inversen, daß das inverse Element von $h \in H$ in H mit dem inversen Element h^{-1} von h in G übereinstimmt. In der Untergruppe H von G stimmt also nicht nur die Operation mit der von G überein, sondern auch das neutrale Element und die Inversen.

2.3.2 UNTERGRUPPENKRITERIUM:
Sei G eine multiplikativ geschriebene Gruppe und sei H eine nichtleere Teilmenge von G , dann gilt:

(1) H ist Untergruppe von G $\Longleftrightarrow \forall a,b \in H \left[ab^{-1} \in H \right]$.

(2) Ist H endlich, dann gilt:
H ist Untergruppe von G $\Longleftrightarrow \forall a,b \in H \left[ab \in H \right]$.

Beweis:
(1)"$\Longrightarrow$": $a,b \in H \Rightarrow a,b^{-1} \in H \Rightarrow ab^{-1} \in H$ nach Definition der Untergruppe.
(1)"$\Longleftarrow$": $a \in H \Rightarrow$ (für $b = a$) $aa^{-1} = e \in H$. Da $e \in H \Rightarrow$ ($a \in H \Rightarrow ea^{-1} = a^{-1} \in H$). Dann folgt aus $a,b \in H$ auch $a,b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$. Damit ist festgestellt, daß die Einschränkung der Gruppenoperation von G auf H eine

Operation in H ist. Da das assoziative Gesetz in ganz G gilt, gilt es auch für die Elemente aus H. Da ferner, wie schon festgestellt, $e \in H$ und für $a \in H$ auch $a^{-1} \in H$, ist H eine Gruppe.

(2)"$\Rightarrow$": Klar.

(2)"$\Leftarrow$": Nach Voraussetzung existiert für jedes $a \in H$ die Abbildung $a^{(\ell)} : H \ni h \mapsto ah \in H$, die nach 2.1.2 injektiv ist. In III.1.4.2 wurde gezeigt, daß eine injektive Abbildung einer endlichen Menge M nach M auch surjektiv ist. Da mit $a \in H$ nach Voraussetzung auch $aa = a^2 \in H$, ist auch $H \ni h \mapsto a^2 h \in H$ surjektiv. Daher gibt es ein $h_o \in H$ mit $a^2 h_o = a$, folglich gilt

$$a^{-2}(a^2 h_o) = h_o = a^{-2}a = a^{-1} \in H ,$$

das heißt, $a \in H$ impliziert $a^{-1} \in H$. Dann folgt $a,b \in H \Rightarrow a,b^{-1} \in H \Rightarrow ab^{-1} \in H$, also ist die Bedingung in (1) erfüllt und folglich gilt (2).//

2.4 Restklassen

2.4.1 DEFINITION:
Seien $H \subsetneq G$ und $a \in H$, dann heißt

$$aH := \{ah \mid h \in H\}$$

bzw.

$$Ha := \{ha \mid h \in H\}$$

die durch a erzeugte R e c h t s - bzw. L i n k s r e s t - k l a s s e von G modulo H oder auch von G nach H.

Wir beschränken uns im folgenden auf die Betrachtung von Rechtsrestklassen, da die entsprechenden Überlegungen für Linksrestklassen völlig analog verlaufen.

2.4.2 HILFSSATZ:
Seien $H \subsetneq G$ und $a,b \in H$, dann gilt:

(1) $aH = bH \Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H$,

(2) $\{aH \mid a \in G\}$ ist eine Partition von G.

Beweis:
(1): $aH = bH \Rightarrow be = b \in aH$ (, da $e \in H$).

Umgekehrt besagt $b \in aH$, daß ein $h_0 \in H$ mit $b = ah_0$ existiert. Es folgt $bH = (ah_0)H = a(h_0H) = aH$, also gilt $aH = bH \iff b \in aH$. Aus $b \in aH$ folgt $b = ah_0$, $h_0 \in H$ und dies impliziert $a^{-1}b = h_0 \in H$. Ist umgekehrt $a^{-1}b = h_0 \in H$, dann folgt $b = ah_0$, also $b \in aH$. Damit ist (1) gezeigt.
(2): Wegen $a \in aH$ folgt $aH \neq \emptyset$ und $\bigcup_{a \in G} aH = G$. Sei $b \in aH \cap cH$ mit $a,b,c \in G$, dann folgt nach (1) $aH = bH = cH$, also sind verschiedene Restklassen disjunkt. Insgesamt ist gezeigt, daß $\{ aH \mid a \in G \}$ eine Partition ist.//

Der erste Teil von (1) besagt, daß genau die Repräsentanten einer Restklasse die Restklasse erzeugen.

Der Beweis dieses Hilfssatzes kann auch so geführt werden, daß man durch

$$a \sim b :\iff a^{-1}b \in H$$

eine Äquivalenzrelation in G definiert, für die die durch a erzeugte Restklasse gleich aH ist. Die Behauptung folgt dann aus III.2.1.3 . Der Leser möge dies zur Übung nachprüfen.

Man beachte bei allen Überlegungen, wie sich die Schreibweise ändert, wenn die Gruppenoperation als Addition geschrieben wird.

Machen wir uns die Situation noch einmal an Beispielen klar.

1) Sei jetzt $G = \mathbb{Z}$ mit der Addition als Gruppenoperation und sei $H = \mathbb{Z}n = \{ zn \mid z \in \mathbb{Z} \}$ mit $n \in \mathbb{N}$. Es gibt jetzt genau die Restklassen

$$0 + \mathbb{Z}n \ , \ 1 + \mathbb{Z}n \ , \ \ldots \ , \ (n-1) + \mathbb{Z}n \ .$$

Siehe auch die Ausführungen zu diesem Beispiel in III.2.1 und III.2.2.

2) Sei jetzt $G = \mathbb{R}$ mit der Addition als Gruppenoperation und $\mathbb{Z}$ als Untergruppe. Überlege, daß man dann genau alle Restklassen in der Form $\varrho + \mathbb{Z}$ mit $0 \leq \varrho < 1$ erhält.

2.5 Die Ordnung einer Gruppe

2.5.1 DEFINITION:
Die O r d n u n g einer Gruppe G , in Zeichen Ord(G) , sei die Elementezahl von G , falls G nur endlich viele Elemente enthält, und sonst das Symbol ∞ .

Beachte, daß die so definierte Ordnung einer Gruppe nichts mit einer Ordnung einer Menge im Sinne von III.3.1.1 zu tun hat.

Ist $Ord(G) = \infty$, so kann die Ordnung von G noch genauer als Kardinalzahl von G definiert werden, doch ist dies hier für uns nicht von Interesse.

2.5.2 SATZ:
Sei G eine Gruppe mit $Ord(G) = n\ (\in \mathbb{N})$ und sei $H \leq G$, dann ist Ord(H) ein Teiler von Ord(G) .

Beweis: Da nach 2.4.2 $\{aH \mid a \in G\}$ eine Partition ist, kann man die Elemente aus G dadurch zählen, daß man die Summe der Anzahlen der Elemente in den verschiedenen aH bildet. Da, wie in 2.1.2 festgestellt,

$$G \ni x \longmapsto ax \in G$$

eine Injektion ist, enthält aH genau so viele Elemente wie H . Ist die Zahl der verschiedenen Restklassen aH gleich m , dann folgt

$$Ord(G) = m\ Ord(H)\ .//$$

Die Anzahl der verschiedenen Restklassen von G nach H nennt man auch den I n d e x von G nach H .

Aus diesem Resultat ergibt sich zum Beispiel die

2.5.3 FOLGERUNG:
Ist G eine Gruppe mit $Ord(G) = p$ = Primzahl , dann besitzt G nur die "trivialen" Untergruppen $\{e\}$ und G .

Beweis: Eine Primzahl p besitzt nur die Teiler 1 und p . Da e in jeder Untergruppe enthalten ist, ist $\{e\}$ die einzige Untergruppe mit einem Element. Ebenso ist G die einzige

Untergruppe mit $Ord(G) = p$ Elementen.//

Als wichtiges Beispiel soll die Ordnung der symmetrischen Gruppe S_n (siehe 2.2.3) bestimmt werden.

2.5.4 SATZ:

$$Ord(S_n) = n! \quad (= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n) .$$

Beweis: Um einen Induktionsbeweis führen zu können, beweisen wir sogleich etwas mehr als die Aussage des Satzes und zwar: Sind A und B beides Mengen mit n Elementen, dann gibt es genau n! Bijektionen von A nach B . Beweis durch Induktion nach n .
Induktionsbeginn $n = 1$: Dann gibt es offensichtlich genau eine Bijektion von A nach B .
Induktionsannahme: Die Behauptung sei für alle Mengen A und B mit n-1 Elementen richtig.
Induktionsschluß: Seien jetzt $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_n\}$ Mengen mit n Elementen und bezeichne $A_i := A \setminus \{a_i\}$ bzw. $B_i := B \setminus \{b_i\}$. Ist α eine Bijektion von A nach B mit $\alpha(a_n) = b_i$, dann ist

$$\alpha' : A_n \ni a \longmapsto \alpha(a) \in B_i$$

eine Bijektion von A_n nach B_i . Umgekehrt kann jede Bijektion $\alpha' : A_n \longrightarrow B_i$ zu einer Bijektion $\alpha : A \longrightarrow B$ durch durch die Festsetzung

$$\alpha(a) := \alpha'(a) \quad \text{für} \quad a \in A_n$$
$$\alpha(a_n) := b_i$$

fortgesetzt werden. Da es nach Induktionsannahme (n-1)! Bijektionen von A_n nach B_i gibt, gibt es auch (n-1)! Bijektionen von A nach B mit $\alpha(a_n) = b_i$. Da dies für jedes $i = 1, \ldots, n$ gilt, ist die Anzahl aller Bijektionen von A nach B gleich $n \cdot (n-1)! = n!$. //

2.6 Normalteiler und Faktorgruppe

Eine Untergruppe H von G mit der Eigenschaft

$$\forall a \in G \left[a^{-1} H a = H \right]$$

hatten wir in 2.3.1 Normalteiler von G genannt. Wir stellen

zunächst fest:

$$a^{-1}Ha = H \iff Ha = aH \quad .$$

Zum Beweis multipliziere man $a^{-1}Ha = H$ von links mit a bzw. $Ha = aH$ von links mit a^{-1}. Bei einem Normalteiler stimmen also die Rechtsrestklassen von G nach H mit den Linksrestklassen von G nach H überein. Aufgrund dieser Voraussetzung ist es nun möglich, die Menge der Restklassen

$$\{aH \mid a \in G\} = \{Ha \mid a \in G\}$$

selbst wieder zu einer Gruppe, der sogenannten F a k t o r g r u p p e oder R e s t k l a s s e n g r u p p e von G nach H , in Zeichen G/H , zu machen. Sei zunächst als Menge

$$G/H := \{aH \mid a \in G\} \quad .$$

2.6.1 BEHAUPTUNG:

$$\bar{\gamma} : (G/H) \times (G/H) \ni (aH, bH) \longmapsto abH \in G/H$$

ist eine Gruppenoperation.

Beweis: Der wesentliche Punkt beim Beweis, bei dem die Normalteilereigenschaft von H eingeht, ist der zu zeigen, daß $\bar{\gamma}$ eine Abbildung ist. Zunächst wäre es ja möglich, daß, wenn man aH und bH durch andere Repräsentanten erzeugt, etwa $aH = a'H$ und $bH = b'H$, man ein von abH verschiedenes Element $a'b'H$ erhalten würde. Aus $aH = a'H$, $bH = b'H$ folgt $a' = ah_1$, $b' = bh_2$ mit $h_1, h_2 \in H$, also gilt

$$a'b'H = ah_1bh_2H$$

Wegen $Hb = bH$ gibt es ein $h_1' \in H$ mit $h_1b = bh_1'$; damit folgt $ah_1bh_2H = abh_1'h_2H = abH$, was zu zeigen war. Um die weiteren Gruppeneigenschaften zu prüfen, setzen wir

$$aH \cdot bH := \bar{\gamma}(aH, bH) = abH \quad .$$

Assoziatives Gesetz: $(aH \cdot bH) \cdot cH = abH \cdot cH = (ab)cH = a(bc)H = aH \cdot bcH = aH \cdot (bH \cdot cH)$.

Neutrales Element: Dies ist eH , denn $eH \cdot aH = eaH = aH = aeH = aH \cdot eH$.

Inverses Element: Das inverse Element von aH ist $a^{-1}H$, denn

$aH \cdot a^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H \cdot aH$.
Damit ist 2.6.1 bewiesen.//

Man beachte, daß gilt

$$aH \cdot bH = abH = aHbH := \{ah_1bh_2 \mid h_1, h_2 \in H\} ,$$

denn $aHbH = a(Hb)H = a(bH)H = abHH = abH$.

2.7 Gruppenhomomorphismen

2.7.1 DEFINITION:
Seien G eine Gruppe mit multiplikativ geschriebener Gruppenoperation und G' eine Gruppe mit der Gruppenoperation $\circ$.

(1) Eine Abbildung $\varphi : G \longrightarrow G'$ heißt ein G r u p p e n h o m o m o r p h i s m u s (oder kurz Homomorphismus) von G nach G' : $\Longleftrightarrow$

$$\forall a,b \in G \left[\varphi(ab) = \varphi(a) \circ \varphi(b) \right] .$$

(2) Ein Gruppenhomomorphismus φ heißt ein E p i m o r p h i s m u s bzw. M o n o m o r p h i s m u s bzw. I s o m o r p h i s m u s , wenn φ surjektiv bzw. injektiv bzw. bijektiv ist. (Siehe dazu auch VI.3) .

(3) Seien $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus und e' das neutrale Element von G' , dann heißt

$$Ke(\varphi) := \{a \mid a \in G \wedge \varphi(a) = e'\}$$

der K e r n von φ .

2.7.2 FOLGERUNG:
Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus, dann gilt:

1) Ist e das neutrale Element von G , dann folgt $e \in Ke(\varphi)$, das heißt $\varphi(e) = e'$.
2) Für alle $a \in G$ gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$.
3) $Ke(\varphi)$ ist ein Normalteiler von G .

Beweis:
1): Aus $\varphi(e) = \varphi(ee) = \varphi(e) \circ \varphi(e)$ folgt nach 2.1.1 , daß $\varphi(e)$ das neutrale Element e' von G' ist.
2): $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e' \Longrightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$.
3): Seien $a \in G$, $k \in Ke(\varphi)$, dann folgt

$$\varphi(a^{-1}ka) = \varphi(a^{-1})\circ\varphi(k)\circ\varphi(a) = \varphi(a^{-1})\circ e'\circ\varphi(a)$$
$$= \varphi(a^{-1})\circ\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e' ,$$

also gilt $a^{-1}Ke(\varphi)a \subset Ke(\varphi)$. Da dies für jedes $a \in G$ gilt, also auch für a^{-1} an Stelle von a , folgt auch

$$Ke(\varphi) = a^{-1}(aKe(\varphi)a^{-1})a \subset a^{-1}Ke(\varphi)a$$

Folglich gilt $a^{-1}Ke(\varphi)a = Ke(\varphi)$, was zu zeigen war.//

Es soll jetzt festgestellt werden, daß jeder Normalteiler H als Kern eines Homomorphismus vorkommt und zwar als Kern des sogenannten natürlichen oder kanonischen Epimorphismus von G auf die Faktorgruppe G/H .

2.7.3 BEHAUPTUNG:
Ist H Normalteiler der (multiplikativ geschriebenen) Gruppe G , dann ist

$$\nu : G \ni a \longmapsto aH \in G/H$$

ein Epimorphismus mit $Ke(\nu) = H$.

Beweis: Daß ν eine surjektive Abbildung ist, ist klar. Wegen

$$\nu(ab) = abH = aH\cdot bH = \nu(a)\cdot\nu(b)$$

ist ν ein Homomorphismus, also ein Epimorphismus. Das neutrale Element von G/H ist $eH = H$. Daher gilt $a \in Ke(\nu) \iff aH = eH = H \iff a \in H$ und folglich $Ke(\nu) = H$ .//

2.7.4 HOMOMORPHIESATZ:
Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann ist

$$\nu : G \ni a \longmapsto aKe(\varphi) \in G/Ke(\varphi)$$

der natürliche Epimorphismus mit $Ke(\nu) = Ke(\varphi)$ und

$$\bar{\varphi} : G/Ke(\varphi) \ni aKe(\varphi) \longmapsto \varphi(a) \in G'$$

ist ein Monomorphismus und es gilt $\varphi = \bar{\varphi}\nu$.

Wir geben für diesen Satz zwei Beweise und zwar einen "direkten" Beweis und einen Beweis, der sich auf die Überlegungen in III.2.3 über Faktorisierung stützt.

1. Beweis: Aus 2.7.2 und 2.7.3 folgt die Behauptung über ν . Für $\bar{\varphi}$ muß zunächst festgestellt werden, daß es eine Abbildung

ist, denn die Definition von $\overline{\varphi}(aH) = \varphi(a)$ hängt von dem Repräsentanten a von aH ab. Sei $aH = bH$, also $b = ah$ mit $h \in H$, dann folgt

$$\varphi(b) = \varphi(ah) = \varphi(a) \circ \varphi(h) = \varphi(a) \circ e' = \varphi(a) \quad ,$$

so daß aus $aH = bH$ folgt

$$\overline{\varphi}(aH) = \varphi(a) = \varphi(b) = \overline{\varphi}(bH) \quad .$$

Somit ist $\overline{\varphi}(aH)$ unabhängig von der Wahl des Repräsentanten a von aH durch aH eindeutig bestimmt, das heißt, $\overline{\varphi}$ ist eine Abbildung. Dafür gilt

$$\overline{\varphi}(aH \cdot bH) = \overline{\varphi}(abH) = \varphi(ab) = \varphi(a) \circ \varphi(b) = \overline{\varphi}(aH) \circ \overline{\varphi}(bH) \quad ,$$

also ist $\overline{\varphi}$ ein Gruppenhomomorphismus. Sei jetzt

$$\overline{\varphi}(aH) = \varphi(a) = \varphi(b) = \overline{\varphi}(bH) \quad ,$$

dann folgt

$$e' = \varphi(a)^{-1} \circ \varphi(b) = \varphi(a^{-1}) \circ \varphi(b) = \varphi(a^{-1}b) \quad ,$$

also $a^{-1}b = k \in H = Ke(\varphi)$, woraus $aH = bH$ folgt. Also ist $\overline{\varphi}$ injektiv, das heißt ein Monomorphismus. Schließlich gilt

$$\overline{\varphi}\nu(a) = \overline{\varphi}(\nu(a)) = \overline{\varphi}(aH) = \varphi(a) \quad ,$$

woraus $\varphi = \overline{\varphi}\nu$ folgt. Damit ist der Beweis vollständig.//

2. Beweis: Sei $\sim$ die zu φ im Sinne von III.2.3 gehörende Äquivalenzrelation. Dafür zeigen wir zuerst

$$G/\sim \; = \; G/Ke(\varphi)$$

(als Gleichung zwischen Mengen). Sei $\overline{a}$ die durch a erzeugte Äquivalenzklasse bezüglich $\sim$, dann ist $\overline{a} = aKe(\varphi)$ zu beweisen:

$$x \in \overline{a} \iff a \sim x \iff \varphi(a) = \varphi(x) \iff$$
$$e' = \varphi(a)^{-1} \circ \varphi(x) = \varphi(a^{-1}) \circ \varphi(x) = \varphi(a^{-1}x) \iff$$
$$a^{-1}x \in Ke(\varphi) \iff x \in aKe(\varphi) \quad .$$

Also gilt tatsächlich $G/\sim \; = G/Ke(\varphi)$ und dann folgt $\varphi = \overline{\varphi}\nu$ wie in III.2.3.4 gezeigt. Wie im ersten Beweis zeigt man schließlich, daß ν und $\overline{\varphi}$ Gruppenhomomorpismen sind.//

Die Bedeutung dieses Satzes liegt darin, daß ν nur von

Ke(φ) abhängt und für alle Normalteiler H von G in der gleichen Weise durch

$$G \ni a \longmapsto aH \in G/H$$

definiert wird. Ferner gilt offensichtlich, daß, wenn φ ein Epimorphismus bzw. ein Monomorphismus ist, $\bar{\varphi}$ bzw. ν sogar ein Isomorphismus ist.

2.8 Beispiel für einen Gruppenisomorphismus

Als Beispiel für einen Gruppenisomorphismus wollen wir jetzt die Bemerkung im Anschluß an 2.2.3 präzisieren, die besagt, daß es zur Definition der symmetrischen Gruppe S_n unwesentlich ist, welche Menge M mit n Elementen zugrunde gelegt wird.

Seien $A = \{a_1,\dots,a_n\}$ und $B = \{b_1,\dots,b_n\}$ zwei Mengen mit je n Elementen. Seien S_n die Permutationsgruppe von A und T_n die von B . Durch

$$\alpha: \quad A \ni a_i \longmapsto b_i \in B$$

wird eine Bijektion definiert, die wir nun benutzen, um einen Gruppenisomorphismus φ zwischen S_n und T_n anzugeben. Sei φ definiert durch

$$\varphi: \quad S_n \ni \pi \longmapsto \alpha\pi\alpha^{-1} \in T_n \quad .$$

Da α , π und α^{-1} Bijektionen sind, ist $\alpha\pi\alpha^{-1}$ eine Permutation von B , also ein Element aus T_n . Wie angegeben, ist daher φ eine Abbildung. Ferner ist φ injektiv: Seien $\pi_1,\pi_2 \in S_n$ mit $\alpha\pi_1\alpha^{-1} = \alpha\pi_2\alpha^{-1}$, so folgt durch Multiplikation dieser Gleichung mit α^{-1} von links und mit α von rechts $\pi_1 = \pi_2$. Da φ injektiv ist, folgt nach III.1.4.1, daß φ auch bijektiv ist. Für $\pi_1, \pi_2 \in S_n$ gilt schließlich

$$\begin{aligned}\varphi(\pi_1\pi_2) &= \alpha\pi_1\pi_2\alpha^{-1} = \alpha\pi_1 1_A \pi_2\alpha^{-1} \\ &= \alpha\pi_1(\alpha^{-1}\alpha)\pi_2\alpha^{-1} = (\alpha\pi_1\alpha^{-1})(\alpha\pi_2\alpha^{-1}) \\ &= \varphi(\pi_1)\varphi(\pi_2) \quad ,\end{aligned}$$

also ist φ ein Gruppenisomorphismus.

2.9 Die von einem kommutativen Monoid erzeugte Gruppe

In 2.2 haben wir schon ein Prinzip kennen gelernt, um aus einem Monoid eine Gruppe zu erhalten, die Gruppe der invertierbaren Elemente. Zu einem Monoid kann eine weitere sehr wichtige Gruppe konstruiert werden. Diese ergibt sich aus dem Problem, zu einem Monoid für nicht invertierbare Elemente Inverse hinzuzufügen. Wir beschränken uns hier auf den kommutativen Fall.

Sei also M ein kommutatives Monoid, dessen Operation als Multiplikation geschrieben wird. Zunächst wird eine Äquivalenzrelation für $M \times M$ definiert. Dazu setze man für $(a,b),(c,d) \in M \times M$:

$$(a,b) \sim (c,d) :\Longleftrightarrow \exists t \in M \,[tad = tbc]$$

Reflexivität: Für das neutrale Element e von M gilt
$eab = eba \Longrightarrow (a,b) \sim (a,b)$.
Symmetrie: Sei $(a,b) \sim (c,d)$ mit $tad = tbc$, dann folgt $tcb = tda$ und dies besagt $(c,d) \sim (a,b)$.
Transitivität: Seien $(a_1,b_1) \sim (a_2,b_2)$, $(a_2,b_2) \sim (a_3,b_3)$
$\Longrightarrow \exists t_1,t_2 \in M \,[t_1a_1b_2 = t_1b_1a_2 \wedge t_2a_2b_3 = t_2b_2a_3]$. Multipliziert man jeweils die linken und die rechten Seiten dieser Gleichungen, so folgt $(t_1t_2a_2b_2)a_1b_3 = (t_1t_2a_2b_2)b_1a_3$, also gilt $(a_1,b_1) \sim (a_3,b_3)$.

Sei nun $G := M \times M/\sim$ die Menge der Äquivalenzklassen dieser Äquivalenzrelation. Die Äquivalenzklasse von (a,b) bezeichnen wir mit $\frac{a}{b}$ (oder mit a-b , wenn M additiv geschrieben wird).

Behauptung: G ist mit folgender Multiplikation

$$\frac{a}{b} \cdot \frac{r}{s} := \frac{ar}{bs}$$

eine kommutative Gruppe.

Beweis: Zunächst ist zu zeigen, daß

$$G \times G \ni \left(\frac{a}{b},\frac{r}{s}\right) \longmapsto \frac{ar}{bs} \in G$$

eine Abbildung ist und dies ist der Fall, wenn $\frac{ar}{bs}$ nicht von der Wahl der Repräsentanten von $\frac{a}{b}$ und $\frac{r}{s}$ abhängt. Sei $(a,b) \sim (a',b')$ und $(r,s) \sim (r',s')$, dann existieren

$t,t' \in M$ mit $tab' = tba'$ und $t'rs' = t'sr'$. Daraus folgt $tt'arb's' = tt'bsa'r'$, also gilt $\frac{ar}{bs} = \frac{a'r'}{b's'}$. Damit hat G die in der Behauptung angegebene Operation. Nun ist leicht zu sehen, daß dabei G eine kommutative Gruppe ist :

$$(\frac{a}{b}.\frac{r}{s}).\frac{u}{v} = \frac{(ar)u}{(bs)v} = \frac{a(ru)}{b(sv)} = \frac{a}{b}.(\frac{r}{s}.\frac{u}{v}) \ ,$$

$$\frac{e}{e}.\frac{r}{s} = \frac{r}{s} = \frac{r}{s}.\frac{e}{e} \quad , \quad (e = \text{neutrales Element von M}) \ ,$$

$$\frac{a}{b}.\frac{b}{a} = \frac{ab}{ab} = \frac{e}{e} \quad , \text{ da } (ab,ab) \sim (e,e) \text{ wegen } eabe = eabe$$

$$\frac{a}{b}.\frac{r}{s} = \frac{ar}{bs} = \frac{ra}{sb} = \frac{r}{s}.\frac{a}{b} \ .$$

Wir erhalten jetzt außerdem ein Monoidhomomorphismus (siehe 1.1.4) $f : M \longrightarrow G$ durch die Definition $f(a) := \frac{a}{e}$. Es ist nämlich $f(e) = \frac{e}{e}$ das neutrale Element von G und

$$f(ab) = \frac{ab}{e} = \frac{ab}{ee} = \frac{a}{e}.\frac{b}{e} = f(a).f(b) \ .$$

Allerdings ist f im allgemeinen nicht injektiv !

2.9.1 HILFSSATZ:
Der Monoidhomomorphismus $f : M \longrightarrow G$ ist genau dann injektiv, wenn die folgende K ü r z u n g s e i g e n s c h a f t gilt:

$$\forall a,b,c \in M \, [ab = ac \implies b = c] \ .$$

Beweis: Sei zuerst f injektiv und gelte $ab = ac$, dann folgt, wie man leicht nachprüft :

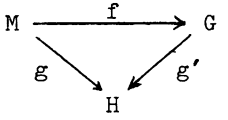
$$f(b) = \frac{b}{e} = \frac{ab}{a} = \frac{ac}{a} = \frac{c}{e} = f(c) \ .$$

Da f injektiv ist, folgt $b = c$. Gelte jetzt die Kürzungsregel und sei $f(b) = f(c)$, also $\frac{b}{e} = \frac{c}{e}$. Dann existiert ein $t \in M$ mit $tb = tbe = tce = tc$. Daraus folgt $b = c$, also ist f injektiv.//

2.9.2 DEFINITION:
Die kommutative Gruppe G zusammen mit dem Monoidhomomorphismus $f : M \longrightarrow G$ heißt die vom kommutativen Monoid M e r z e u g t e kommutative Gruppe.

Sie besitzt eine sogenannte "universelle" Eigenschaft, durch die sie auch häufig definiert wird. Dies zeigt der folgende

2.9.3 SATZ:
Seien M ein kommutatives Monoid und (G,f) die von M erzeugte kommutative Gruppe. Seien H eine weitere kommutative Gruppe und $g : M \longrightarrow H$ ein Monoidhomomorphismus. Dann existiert genau ein Gruppenhomomorphismus $g' : G \longrightarrow H$, so daß



kommutativ ist, also $g = g'f$ gilt.

Beweis: Die Gruppenoperation von H wird wie die von G als Multiplikation geschrieben. Sei die Abbildung g_1 definiert durch

$$g_1 : M \times M \longrightarrow H \quad , \quad g_1(a,b) := g(a)g(b)^{-1} .$$

Ist $(a,b) \sim (a',b')$, also $tab' = tba'$, so folgt $tab^{-1} = ta'b'^{-1}$ und daher gilt

$$g(t)g(a)g(b)^{-1} = g(t)g(a')g(b')^{-1}.$$

Da H eine Gruppe ist, kann diese Gleichung durch $g(t)$ "gekürzt" werden und dann folgt $g_1(a,b) = g_1(a',b')$. Nach III.2.3.1 gibt es genau eine Abbildung $g' : G \longrightarrow H$ mit $g'(\frac{a}{b}) = g_1(a,b)$. Außerdem gilt

$$g'(\tfrac{a}{b}\cdot\tfrac{r}{s}) = g'(\tfrac{ar}{bs}) = g(ar)g(bs)^{-1} = g(a)g(b)^{-1}g(r)g(s)^{-1}$$
$$= g'(\tfrac{a}{b})g'(\tfrac{r}{s}) \quad ,$$

also ist g' ein Gruppenhomomorphismus. Für $a \in M$ gilt

$$g'f(a) = g'(\tfrac{a}{e}) = g(a)g(e)^{-1} = g(a) \quad ,$$

also $g'f = g$. Sei nun $h : G \longrightarrow H$ ein weiterer Gruppenhomomorphismus mit $hf = g$. Dann ist $h(\frac{a}{e}) = hf(a) = g(a)$ und

$$h(\tfrac{e}{a})g(a) = h(\tfrac{e}{a})h(\tfrac{a}{e}) = h(\tfrac{a}{a}) = h(e) \quad .$$

$h(e)$ ist aber das neutrale Element von H, so daß

$$h(\tfrac{e}{a}) = g(a)^{-1}$$

folgt. Damit erhält man

$$h(\tfrac{a}{b}) = h(\tfrac{a}{e})h(\tfrac{e}{b}) = g(a)g(b)^{-1} = g'(\tfrac{a}{b}) \quad ,$$

also gilt $h = g'$ .//

§ 3 Ringe

3.1 Allgemeine Eigenschaften

Die bisher betrachteten algebraischen Strukturen wie Halbgruppen, Monoide und Gruppen sind durch eine (binäre) Operation, die gewisse Bedingungen erfüllen muß, definiert. In den Ringen und Körpern lernen wir algebraische Strukturen kennen, die durch zwei Operationen - eine Addition und eine Multiplikation - definiert werden.

3.1.1 DEFINITION:
Ein **Ring** ist ein Tripel $(R,+,\cdot)$ mit folgenden Eigenschaften:
(1) $(R,+)$ ist eine kommutative Gruppe.
(2) $(R,\cdot)$ ist eine Halbgruppe.
(3) Es gelten die distributiven Gesetze:
$\forall a,b,c \in R \left[(a+b)c = ac + bc \wedge a(b+c) = ab + ac\right]$.

$(R,+,\cdot)$ heißt ein Ring mit 1-Element, falls $(R,\cdot)$ ein Monoid ist.

$(R,+,\cdot)$ heißt ein **kommutativer Ring**, falls $(R,\cdot)$ kommutativ ist.

$(R,+,\cdot)$ heißt **nullteilerfrei**, wenn gilt
$\forall a,b \in R \left[ab = 0 \Longrightarrow a = 0 \vee b = 0\right]$.

Wir geben jetzt eine Reihe von Bezeichnungen, Bemerkungen und Folgerungen an, die wir später meist ohne besonderen Hinweis benutzen werden.

Die Operation $+$ wird Addition genannt, $a+b$ heißt **Summe** von a und b und wird auch als "a plus b" gelesen. Das neutrale Element bei der Addition, das,wie früher festgestellt, eindeutig bestimmt ist, wird **Nullelement** oder kurz **Null** genannt und mit 0 bezeichnet. Die Operation $\cdot$ wird **Multiplikation** genannt, $a\cdot b$ oder ab heißt **Produkt** von a und b und wird auch als "a mal b" gelesen. Hat $(R,\cdot)$ ein neutrales Element, das ebenfalls eindeutig bestimmt ist,

so wird dieses E i n s e l e m e n t oder kurz E i n s genannt und mit 1 bezeichnet. Bei diesen Bezeichnungen beachte man aber, daß im allgemeinen 0 und 1 keine Zahlen sind (es sei denn, R ist ein Zahlring) .

Wir geben jetzt eine Reihe von einfachen Folgerungen aus der Definition an.

3.1.2 BEHAUPTUNG:
$\forall r \in R \; [r0 = 0r = 0]$.

Beweis: Aus $0 = 0 + 0$ folgt $r0 = r(0 + 0) = r0 + r0$ $\Longrightarrow 0 = r0 - r0 = r0 + r0 - r0 = r0 + 0 = r0$. Analog folgt die andere Seite. //

Sei jetzt 0 ein Symbol und setzt man $0 + 0 := 0$, $00 := 0$, dann wird dadurch ein Ring mit genau einem Element, nämlich 0 , definiert. Ist andrerseits R ein Ring mit genau einem Element, so muß dieses das Nullelement 0 der Addition sein, da dieses nach Voraussetzung ($(R,+)$ ist Gruppe) existieren muß. Es gilt dann ebenfalls $0 + 0 = 0$, $00 = 0$. Es gibt also bei unserer Bezeichnung genau einen Ring mit genau einem Element, dieser wird als N u l l r i n g bezeichnet. Beachte: Der Nullring ist ein Ring mit Einselement ($= 0$) .

3.1.3 BEHAUPTUNG:
In einem Ring R mit Einselement, der mindestens zwei Elemente besitzt, gilt $1 \neq 0$.

Beweis: Sei $r \in R$, $r \neq 0$. Angenommen $1 = 0$, dann folgt nach 3.1.2 $r = r1 = r0 = 0$. Widerspruch! //

3.1.4 BEHAUPTUNG:
$\forall r,s \in R \; [r(-s) = (-r)s = -(rs)]$.

Beweis: $rs + r(-s) = r(s + (-s)) = r0 = 0$.
Wegen der Eindeutigkeit des inversen Elements in einer Gruppe folgt $r(-s) = -(rs)$. Analog schließt man für $(-r)s$. //

3.2 Homomorphismen und Ideale

Abbildungen von Ringen, die die Struktur des Ringes "erhalten", heißen Homomorphismen. Genauer gilt

3.2.1 DEFINITION:

1) Seien R und S Ringe. Eine Abbildung

$$\varphi: R \longrightarrow S$$

heißt (Ring-)Homomorphismus von R nach S $:\Longleftrightarrow$

a) φ ist ein Homomorphismus der additiven Gruppe von R in die von S, d.h.
$\forall r_1, r_2 \in R \left[\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)\right]$,

b) $\forall r_1, r_2 \in R \left[\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)\right]$.

2) Ein Ringhomomorphismus $\varphi: R \longrightarrow S$ heißt unitär $\Longleftrightarrow$ R und S sind Ringe mit Einselement 1 bzw. $1'$ und es gilt $\varphi(1) = 1'$.

3) Sei $\varphi: R \longrightarrow S$ ein Ringhomomorphismus. Dann heißt

$$Ke(\varphi) := \{k \mid k \in R \wedge \varphi(k) = 0 \in S\}$$

der Kern von φ.

4) Eine Teilmenge C eines Ringes R heißt Linksideal bzw. Rechtsideal bzw. zweiseitiges Ideal von R $:\Longleftrightarrow$

a) C ist Untergruppe der additiven Gruppe von R

b) $\forall c \in C \, \forall r \in R \left[rc \in C \text{ bzw. } cr \in C \text{ bzw. } cr \in C \wedge rc \in C\right]$.

Die weiteren Überlegungen sollen zeigen, daß der Kern eines Ringhomomorphismus ein zweiseitiges Ideal ist und daß umgekehrt zu jedem zweiseitigen Ideal C ein Ringhomomorphismus angegeben werden kann, dessen Kern gleich C ist.

3.2.2 BEHAUPTUNG:

Ist $\varphi: R \longrightarrow S$ ein Ringhomomorphismus, dann gilt:

a) Ist 0 bzw. $0'$ die Null in R bzw. in S, dann folgt $\varphi(0) = 0'$.

b) $\forall r \in R \left[\varphi(-r) = -\varphi(r)\right]$.

Beweis:

a) $\varphi(0) + \varphi(0) = \varphi(0 + 0) = \varphi(0) \Longrightarrow \varphi(0) = 0'$.

b) $\varphi(r) + \varphi(-r) = \varphi(r - r) = \varphi(0) = 0' \Longrightarrow \varphi(-r) = -\varphi(r)$. //

3.2.3 BEHAUPTUNG:
Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, dann ist $Ke(\varphi)$ ein zweiseitiges Ideal von R .

Beweis: Wegen 3.2.2 gilt $0 \in Ke(\varphi)$, also $Ke(\varphi) \neq \emptyset$.
Ferner folgt aus 3.2.2 für beliebige $k_1, k_2 \in Ke(\varphi)$:

$$\varphi(k_1 - k_2) = \varphi(k_1) - \varphi(k_2) = 0' - 0' = 0' \in S ,$$

also $k_1 - k_2 \in Ke(\varphi)$. Nach dem Untergruppenkriterium ist folglich $Ke(\varphi)$ eine Untergruppe von $(R,+)$.
Seien jetzt $k \in Ke(\varphi)$, $r \in R$, dann gilt

$$\varphi(kr) = \varphi(k)\varphi(r) = 0'\varphi(r) = 0' ,$$

$$\varphi(rk) = \varphi(r)\varphi(k) = \varphi(r)0' = 0' .$$

Damit ist der Beweis vollständig. //

3.3 Restklassenringe

Um nun zu zeigen, daß jedes zweiseitige Ideal Kern eines Homomorphismus ist, konstruieren wir den Restklassen- oder Faktorring nach einem zweiseitigen Ideal. Sei also C zweiseitiges Ideal des Ringes R , dann existiert zunächst die additive Faktorgruppe R/C (im Sinne von 2.6.1), bei der die Addition durch

$$(r_1 + C) + (r_2 + C) := (r_1 + r_2) + C$$

definiert ist.

3.3.1 BEHAUPTUNG:
Definiert man in R/C eine Multiplikation durch

$$(r_1 + C)(r_2 + C) := r_1 r_2 + C ,$$

dann wird R/C zu einem Ring .

Beweis: Stellen wir dazu zuerst fest, daß

$$R/C \times R/C \ni (r_1 + C, r_2 + C) \longmapsto r_1 r_2 + C \in R/C$$

eine Abbildung ist. Sei

$$r_1 + C = r_1' + C \quad , \quad r_2 + C = r_2' + C \quad ,$$

also $r_1' = r_1 + c_1$, $r_2' = r_2 + c_2$,
dann folgt

$$\begin{aligned} r_1'r_2' + C &= (r_1 + c_1)(r_2 + c_2) + C \\ &= r_1r_2 + c_1r_2 + r_1c_2 + c_1c_2 + C \\ &= r_1r_2 + C \quad , \end{aligned}$$

denn da C zweiseitiges Ideal ist, gilt

$$c_1r_2 + r_1c_2 + c_1c_2 \in C \quad .$$

Also hängt $r_1r_2 + C$ nicht von der Wahl der Repräsentanten von $r_1 + C$ und $r_2 + C$ ab, d.h. wir haben in der Tat eine Operation. Wegen

$$\begin{aligned} (r_1 + C)((r_2 + C)(r_3 + C)) &= r_1(r_2r_3) + C \\ &= (r_1r_2)r_3 + C = ((r_1 + C)(r_2 + C))(r_3 + C) \end{aligned}$$

ist diese Operation assoziativ. Ferner gilt

$$\begin{aligned} ((r_1 + C) + (r_2 + C))(r_3 + C) &= (r_1 + r_2 + C)(r_3 + C) \\ &= (r_1 + r_2)r_3 + C \\ &= (r_1r_3 + C) + (r_2r_3 + C) \\ &= (r_1 + C)(r_3 + C) + (r_2 + C)(r_3 + C) \quad , \end{aligned}$$

analog folgt das zweite distributive Gesetz. Ist R ein Ring mit Einselement 1 , dann gilt

$$(r + C)(1 + C) = r1 + C = r + C \quad ,$$

$$(1 + C)(r + C) = 1r + C = r + C \quad ,$$

d.h. dann ist $1 + C$ Einselement von R/C . //
Wir fassen zusammen.

3.3.2 SATZ:
Sei R ein Ring und C ein zweiseitiges Ideal in R . Dann wird die Menge $R/C = \{r + C \mid r \in R\}$ durch die Definitionen

$$\begin{aligned} (r_1 + C) + (r_2 + C) &:= r_1 + r_2 + C \\ (r_1 + C)(r_2 + C) &:= r_1r_2 + C \end{aligned} \qquad (r_1, r_2 \in R)$$

zu einem Ring.

Besitzt R ein Einselement 1, dann ist $1+C$ Einselement des Ringes R/C.

3.3.3 DEFINITION:
Der in 3.3.2 definierte Ring R/C heißt **Faktorring** oder **Restklassenring** von R nach C oder von R **modulo** C.

3.3.4 SATZ:
Voraussetzungen wie in 3.3.2.
Die Abbildung

$$\nu: R \ni r \longmapsto r+C \in R/C$$

ist ein Ringhomomorphismus mit $Ke(\nu) = C$.

Beweis: $\nu(r_1 + r_2) = r_1 + r_2 + C = (r_1 + C) + (r_2 + C)$
$= \nu(r_1) + \nu(r_2)$,

$\nu(r_1 r_2) = r_1 r_2 + C = (r_1 + C)(r_2 + C) = \nu(r_1)\nu(r_2)$,

also ist ν ein Ringhomomorphismus.
Für $c \in C$ folgt $\nu(c) = c + C = C = 0+C$, also $c \in Ke(\nu)$.
Sei umgekehrt $k \in Ke(\nu)$, dann folgt

$$\nu(k) = k + C = 0 + C ,$$

also $k \in C$. Somit gilt $Ke(\nu) = C$. //

Wir wollen jetzt einige Beispiele für Ringe und Ideale betrachten.

3.4 Der Ring der ganzen Zahlen

Die Menge der ganzen Zahlen zusammen mit der üblichen Addition und Multiplikation von ganzen Zahlen ist ein Ring, der der **Ring der ganzen Zahlen** genannt und mit $\mathbb{Z}$ bezeichnet wird (vgl. VII.2). Wir wollen alle Ideale von $\mathbb{Z}$ bestimmen, wobei wir jetzt nicht zwischen Links-, Rechts- und zweiseitigen Idealen unterscheiden müssen, da der Ring $\mathbb{Z}$ kommutativ ist.

Ist r_o Element eines beliebigen Ringes R, dann ist die Menge

$$r_oR := \{r_or \mid r \in R\}$$

ein Rechtsideal von R, wie man leicht nachprüft. Ein solches Ideal, das aus den Vielfachen eines Elementes besteht, heißt ein H a u p t i d e a l. Ein kommutativer Ring, in dem jedes Ideal Hauptideal ist, heißt H a u p t i d e a l r i n g .

3.4.1 SATZ:
$\mathbb{Z}$ ist ein Hauptidealring.

Beweis: Sei C ein Ideal aus $\mathbb{Z}$. Ist $C = \{0\}$, dann folgt $C = 0\mathbb{Z}$. Sei nun $C \neq \{0\}$, dann gibt es ein $c \in C$, $c \neq 0$. Aus $c \neq 0$ folgt $c > 0$ oder $-c > 0$. Da mit $c \in C$ auch $(-1)c = -c \in C$, folgt

$$C^+ := C \cap \mathbb{N} \neq \emptyset .$$

Da die Ordnung von $\mathbb{N}$ eine Wohlordnung ist (siehe VII.1.4.2), gibt es in C^+ ein kleinstes Element c_o. Sei jetzt $z \in \mathbb{Z}$, dann kann z durch c_o mit Rest geteilt werden(siehe VII.2.2.6):

$$z = c_oq + r , \quad q,r \in \mathbb{Z} , \quad 0 \leq r < c_o .$$

Sei jetzt $z \in C$, dann folgt

$$z - c_oq = r \in C .$$

Wegen $r < c_o$ folgt $r \notin C^+$ und wegen $0 \leq r$ folgt $r = 0$, d.h. $z = c_oq$. Damit ist $C \subset c_o\mathbb{Z}$ gezeigt. Wegen $c_o \in C$ gilt aber auch $c_o\mathbb{Z} \subset C$, also $C = c_o\mathbb{Z}$, was zu zeigen war. //

Nachdem wir wissen, daß $\mathbb{Z}$ Hauptidealring ist, können wir alle Restklassenringe von $\mathbb{Z}$ angeben. Diese sind von der Form $\mathbb{Z}/n\mathbb{Z}$ mit $n \in \mathbb{N}_o$ (siehe 3.3.3). Wie im Anschluß an 3.2.4 festgestellt hat $\mathbb{Z}/n\mathbb{Z}$ für $n = 1$ genau die n Elemente $\overline{0},\ldots,\overline{n-1}$, wobei

$$\overline{i} = i + n\mathbb{Z} = \{i + nz \mid z \in \mathbb{Z}\}$$

gilt. Für $n = 0$ gilt $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.

Wir ziehen nun eine wichtige Folgerung aus 3.4.1.

3.4.2 FOLGERUNG:
Seien $m,n \in \mathbb{Z}$ und sei $t \in \mathbb{Z}$ größter gemeinsamer Teiler von m und n. Dann gibt es $a,b \in \mathbb{Z}$ mit

$$ma + nb = t .$$

Beweis: Wie leicht zu sehen, ist

$$m\mathbb{Z} + n\mathbb{Z} := \{mz_1 + nz_2 \mid z_1, z_2 \in \mathbb{Z}\}$$

ein Ideal in $\mathbb{Z}$. Folglich existiert ein $t \in \mathbb{Z}$ mit

$$t\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} .$$

Wegen $m,n \in t\mathbb{Z}$ ist t gemeinsamer Teiler von m und n. Sei auch d gemeinsamer Teiler von m und n, dann gilt $m,n \in d\mathbb{Z}$ und folglich auch

$$t\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z} .$$

Daraus folgt, daß d auch Teiler von t ist, d.h. t ist größter gemeinsamer Teiler von m und n. Wegen $t\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ gibt es $a,b \in \mathbb{Z}$ mit $t = ma + nb$. //

Als Spezialfall ist darin enthalten, daß es zu teilerfremden ganzen Zahlen m und n ganze Zahlen a,b mit $ma + nb = 1$ gibt.

Bekanntlich heißt eine natürliche Zahl $p > 1$ eine P r i m z a h l, wenn p nur die trivialen Teiler 1 und p (in $\mathbb{N}$) besitzt. Die Folge der Primzahlen beginnt mit 2, 3, 5, 7, 11, 13, 17, 19, 23, ... und man weiß seit Euklid, daß es unendlich viele Primzahlen gibt. Über die Verteilung der Primzahlen in der Folge aller natürlichen Zahlen gibt der sogenannte Primzahlsatz eine gewisse Auskunft. (Er besagt, daß die Anzahl der Primzahlen $\leq n$ asymptotisch für $n \longrightarrow \infty$ gleich $\frac{n}{\log n}$ ist.)

Die Grundlage der Arithmetik der ganzen Zahlen

bildet der Satz von der eindeutigen Primzahlzerlegung, der jetzt bewiesen werden soll. Zur Vorbereitung dient die folgende Feststellung.

3.4.3 BEHAUPTUNG:
Sei $p \in \mathbb{N}$, $p > 1$.
Primzahl $p \iff \forall a,b \in \mathbb{N}\,[p/ab \Longrightarrow p/a \vee p/b]$.

Beweis:
$\Longrightarrow$: Gelte $p/ab \wedge p \not/ a$. Da p Primzahl ist, folgt aus $p \not/ a$, daß p und a teilerfremd sind. Nach 3.4.2 existieren dann $x,y \in \mathbb{Z}$ mit

$$px + ay = 1 \ .$$

Durch Multiplikation mit b folgt

$$pxb + aby = b \ .$$

Wegen p/ab folgt daraus p/b , was zu zeigen war.
$\Longleftarrow$: Sei a/p , $a \in \mathbb{N}$. Dann existiert $b \in \mathbb{N}$ mit $p = ab$. Nach Voraussetzung folgt $p/a \vee p/b$. Daraus folgt (wegen $a \neq p$, $b \neq p$) $p = a$ oder $p = b$, und im Falle $p = b$ folgt $a = 1$. //

3.4.4 FOLGERUNG:
Ist p Primzahl und gilt $p/a_1 \ldots a_n$ mit $a_1,\ldots,a_n \in \mathbb{N}$, dann folgt

$$p/a_1 \vee p/a_2 \vee \ldots \vee p/a_n \ .$$

Beweis: Induktion über n , wobei der Induktionsbeginn $n = 2$ durch 3.4.3 geleistet wird. //

3.4.5 SATZ von der eindeutigen Primzahlzerlegung:
Jede natürliche Zahl $n > 1$ ist Produkt von Primzahlen und diese Produktdarstellung ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.

Beweis: 1. Existenz der Zerlegung:
Beweis durch Induktion nach n . Beginn $n = 2$: Behauptung ist erfüllt. Annahme: Die Behauptung sei für alle $a \in \mathbb{N}$ mit $2 \leq a < n$ erfüllt. Schluß: Ist n eine Primzahl, dann ist die Behauptung erfüllt. Ist n keine Primzahl, dann existiert eine Zerle-

gung $n = ab$ mit $2 \leq a < n$, $2 \leq b < n$ und die Behauptung folgt aus der Induktionsannahme für beide Faktoren.

2. Eindeutigkeit der Zerlegung:
Wie zuvor Induktion über n . Sei im Induktionsschluß

$$n = p_1 \cdots p_s = q_1 \cdots q_t$$

mit Primzahlen p_i, q_j . Wegen 3.4.4 teilt p_1 eine der Primzahlen q_j , etwa q_1 (durch Umnumerierung!); da p_1 und q_1 Primzahlen sind, folgt $p_1 = q_1$. Für $p_2 \cdots p_s$ $q_2 \cdots q_t$ gilt dann die Eindeutigkeit nach Induktionsannahme. //

Wir bemerken schließlich noch, daß sich das Resultat von den natürlichen Zahlen auf negative ganze Zahlen überträgt: Ist $z < -1$, dann gilt $z = -p_1 \cdots p_s$ mit eindeutig bestimmten Primzahlen p_i.

3.5 Konstruktion des Polynomringes

Sei R ein Ring mit Einselement und sei $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ (mit $0 \in \mathbb{Z}$) .

Mit $\mathrm{Abb}(\mathbb{N}_0, R)$ wird die Menge aller Abbildungen von $\mathbb{N}_0$ nach R bezeichnet. Sei dann

$$R[X] = \left\{ \varphi \mid \varphi \in \mathrm{Abb}(\mathbb{N}_0, R) \wedge \exists k \in \mathbb{N}_0 \forall i \in \mathbb{N}_0 [i > k \Rightarrow \varphi(i) = 0] \right\}.$$

d.h. die Teilmenge aller Abbildungen von $\mathbb{N}_0$ nach R mit $\varphi(i) \neq 0$ nur für höchstens endlich viele $i \in \mathbb{N}_0$. Schreibt man φ in der Form

$$(r_i) = (r_0, r_1, r_2, \ldots) \quad , \quad \text{mit} \quad r_i := \varphi(i) \quad , \quad i \in \mathbb{N}_0,$$

dann sind also von einer Stelle k ab alle $r_i = 0$.

In $R[X]$ wird durch

$$(a_i) + (b_i) := (a_i + b_i)$$

und

$$(a_i)(b_i) := (c_0, c_1, c_2, \ldots)$$

mit

$$c_l = \sum_{i=0}^{l} a_i b_{l-i} \quad , \quad l \in \mathbb{N}_0$$

eine Addition und Multiplikation eingeführt. Wie leicht nachzuprüfen, wird $R[X]$ damit zu einem Ring mit dem Nullelement $(0,0,0,\ldots)$ und dem Einselement $(1,0,0,\ldots)$.
Setzt man noch für $r \in R$ und $(a_i) \in R[X]$

$$r(a_i) := (ra_i)$$

$$X := (0,1,0,0,0,\ldots)$$

$$X^0 := (1,0,0,0,\ldots) \ ,$$

dann gilt, wie leicht zu prüfen,

$$(r_0,r_1,\ldots,r_k,0,0,\ldots) = \sum_{i=0}^{k} r_i X^i \quad .$$

Meist wird auch noch $rX^0 = r$, $r \in R$ gesetzt, so daß

$$(r_0,r_1,\ldots,r_k,0,0,\ldots) = r_0 + r_1 X + \ldots + r_k X^k$$

gilt. Der rechts stehende Ausdruck heißt ein Polynom in X . Im Falle $r_k \neq 0$ ist das Polynom (durch das gegebene Element aus $R[X]$) eindeutig bestimmt; k heißt dann der G r a d des Polynoms. Für das Nullelement $(0,0,\ldots)$ schreibt man 0 und nennt es das N u l l p o l y n o m ; als Grad wird ihm das Symbol $-\infty$ zugeordnet. Den Ring $R[X]$ nennt man nun den P o l y n o m r i n g in der U n b e s t i m m t e n X mit K o e f f i z i e n t e n in R . Man beachte dabei die irreführende Bezeichnung "Unbestimmte X" da doch X durch $X = (0,1,0,0,\ldots)$ wohldefiniert ist.

Betrachtet man die Abbildung

$$R \ni r \longmapsto (r,0,0,0,\ldots) = rX^0 \in R[X] \quad ,$$

so sieht man sofort, daß diese ein injektiver Ringhomomorphismus ist. Wie schon durch die Schreibweise $r = rX^0$ angegeben, wird R meistens mit RX^0 identifiziert, so daß dann R als Unterring von $R[X]$ betrachtet wird.

3.6 Boolesche Ringe

Um zu zeigen, welche zunächst etwas pathologisch erscheinende Eigenschaften ein Ring haben kann, betrachten wir Boolesche Ringe.

3.6.1 DEFINITION:
Ein Ring R heißt **Boolescher Ring** $:\Longleftrightarrow$

$$\forall r \in R \left[r^2 = r \right] .$$

3.6.2 FOLGERUNG:
Sei R ein Boolescher Ring, dann gilt

$$\forall r \in R \left[r + r = 0 \right]$$

und R ist kommutativ.

Beweis: Seien $r,s \in R \Longrightarrow$
$r + s = (r + s)^2 = r^2 + rs + sr + s^2 = r + s + rs + sr \Longrightarrow$
$rs + sr = 0$. Für $s = r$ folgt $0 = r^2 + r^2 = r + r$.
Also gilt $r = -r$ für jedes Element $r \in R$. Damit folgen aus $rs + sr = 0$ durch Addition von rs:
$sr = 0 + sr = rs + rs + sr = rs + 0 = rs$, also ist R kommutativ. //

Beispiele für Boolesche Ringe erhält man auf folgende Weise. Sei M eine beliebige Menge und sei $P(M)$ die Potenzmenge von M . In $P(M)$ werden eine Addition und eine Multiplikation folgendermaßen eingeführt: Für $r,s \in P(M)$ sei

$$r + s := (r \cup s) \setminus (r \cap s)$$

$$rs := r \cap s .$$

Man prüft leicht nach, daß damit $P(M)$ ein Boolescher Ring ist. Das Nullelement dieses Ringes ist die leere Menge $\emptyset$ und das Einselement die Menge M .

§ 4 Boolesche Algebren

4.1 Definition und Beispiele

Wir geben jetzt eine algebraische Struktur an, die zunächst wie ein Ring aussieht, jedoch kein Ring ist. Es handelt sich um Boolesche Algebren, die in engem Zusammenhang mit den zuvor betrachteten Booleschen Ringen und den in III.3.5.3 eingeführten Booleschen Verbänden stehen. Sie sind insbesondere im Hinblick auf gewisse Anwendungen von Interesse.

4.1.1 DEFINITION:
Ein Quadrupel $(A, \#, \circ, ')$ heißt eine Boolesche Algebra, wenn folgendes gilt:
(I) A ist eine Menge,
(II) $\#$ und $\circ$ sind binäre Operationen von A,
(III) $'$ ist eine Abbildung:

$$': A \ni a \longmapsto a' \in A$$

und für alle $a,b,c \in A$ gelten:

(1) $(a \# b) \# c = a \# (b \# c)$, $(a \circ b) \circ c = a \circ (b \circ c)$

(2) $a \circ (b \# c) = (a \circ b) \# (a \circ c)$, $a \# (b \circ c) = (a \# b) \circ (a \# c)$

(3) $a \# b = b \# a$, $a \circ b = b \circ a$

(4) Es gibt ein Element $\mathcal{O}$ (Nullelement genannt) und ein Element e (Einselemnt genannt) mit

$$a \# \mathcal{O} = a \quad , \quad a \circ e = a \quad .$$

(5) $a \# a' = e$, $a \circ a' = \mathcal{O}$.

Es erhebt sich zunächst die Frage, ob dies ein Ring ist, sind doch insbesondere die assoziativen, kommutativen und (sogar zwei!) distributiven Gesetze erfüllt und es gibt ein Null- und ein Einselement! Was fehlt also, daß A kein Ring ist? Nun, es fehlt die Voraussetzung, daß A bei $\#$ eine Gruppe ist. Es gilt sogar

4.1.2 BEMERKUNG:
Eine Boolesche Algebra, die bezüglich $\#$ und $\circ$ ein Ring ist, besteht nur aus einem Element.

Beweis: Setzt man in (3) (rechts) $b = a$ und $c = a'$, dann folgt $a = a \# 0 = a \# (a \circ a') = (a \# a) \circ (a \# a') = (a \# a) \circ e = a \# a$. Da es nach Voraussetzung jetzt zu a ein inverses Element $(-a)$ bezüglich $\#$ gibt, so daß $a \# (-a)$ das eindeutig bestimmte neutrale Element der Gruppe $(A, \#)$ ist, folgt aus $a = a \# a$ sofort $a \# (-a) = (a \# a) \# (-a) = a \# (a \# (-a)) = a$, folglich ist jedes Element $a \in A$ gleich dem neutralen Element von $(A, \#)$, d.h. A besteht nur aus einem Element. //

Ein Beispiel für eine Boolesche Algebra hat man in der Potenzmenge $P(M)$ zu einer beliebigen Menge M , wenn man für $a,b,c \in P(M)$ setzt:

$$a \# b := a \cup b$$

$$a \circ b := a \cap b$$

$$\sigma := \emptyset$$

$$e := M$$

$$a' := M \setminus a \quad .$$

Dieses Beispiel kann noch verallgemeinert werden, indem man eine nichtleere Teilmenge A von $P(M)$ betrachtet, die mit $a,b \in A$ auch $a \cup b$, $a \cap b$ und $M \setminus a$ enthält. Derartige Boolesche Algebren werden auch M e n g e n k ö r p e r genannt und spielen in der Wahrscheinlichkeitstheorie eine grundlegende Rolle.

4.2 Zusammenhang mit Booleschen Verbänden und Booleschen Ringen

In III.3.5.3 hatten wir Boolesche Verbände kennengelernt und es soll jetzt festgestellt werden, in welcher Beziehung diese zu den Booleschen Algebren stehen.

4.2.1 SATZ:

a) Ist $(A, \#, \circ, ')$ eine Boolesche Algebra, dann wird für $a,b \in A$ durch

$$a \leq b :\Longleftrightarrow a = a \circ b$$

in A eine Ordnung definiert, bei der $(A, \leq)$ ein Boolescher Verband (III.3. .3) ist, und es gilt

(1) $a \cap b = a \circ b$

(2) $a \cup b = a \# b$

(3) Das kleinste bzw. größte Element aus $(A, \leq)$ ist das Nullelement o bzw. das Einselement e aus $(A, \#, \circ, ')$.

b) Ist umgekehrt $(A, \leq)$ ein Boolescher Verband, dann wird durch

$$a \# b := a \cup b$$

$$a \circ b := a \cap b$$

$$a' := a'$$

eine Boolesche Algebra $(A, \#, \circ, ')$ definiert, bei der das Nullelement bzw. Einselement das kleinste bzw. größte Element von $(A, \leq)$ ist.

Beweis bleibt dem Leser als Übung überlassen.

Boolesche Algebren und Boolesche Verbände unterscheiden sich also nur dadurch, daß man einerseits $a \# b$ und $a \circ b$ als algebraische Operationen und andrerseits in der Schreibweise $a \cap b$ und $a \cup b$ als durch eine entsprechende Ordnung definiertes Supremum bzw. Infimum von $\{a,b\}$ betrachtet. Im ersten Fall handelt es sich um eine algebraische Struktur und im zweiten um eine Ordnungsstruktur. Dies zeigt, daß Strukturen, die zunächst sehr unterschiedlich aussehen, doch im Wesentlichen das gleiche mathematische Objekt liefern können. Es ist eine der Hauptaufgaben der Theorie der Kategorien (siehe VI. Kapitel), die Untersuchung ver-

schiedener Strukturen auf gemeinsame Eigenschaften hin zu ermöglichen. Der entscheidende Begriff dafür ist der des Funktors.

Wir gehen jetzt auf den Zusammenhang zwischen Booleschen Algebren und Booleschen Ringen (3.6) ein.

4.2.2 SATZ:

a) Ist $(A,+,\cdot)$ ein Boolescher Ring mit dem Einselement 1, dann wird durch

$$a \# b := a + b + ab$$

$$a \circ b := a.b$$

$$a' := 1 + a$$

eine Boolesche Algebra $(A, \#, \circ, ')$ mit gleichem Eins- und Nullelement wie $(A,+,\cdot)$ definiert.

b) Ist umgekehrt $(A, \#, \circ, ')$ eine Boolesche Algebra, dann wird durch

$$a + b := (a \circ b') \# (a' \circ b)$$

$$a \cdot b := a \circ b$$

ein Boolescher Ring $(A,+,\cdot)$ mit gleichem Eins- und Nullelement wie $(A, \#, \circ, ')$ definiert.

Beweis: Übung für den Leser.

Bemerkenswert ist ferner noch, daß man bei den Übergängen

$$(A,+,\cdot) \xrightarrow{a)} (A, \#, \circ, ') \xrightarrow{b)} (A,+,\cdot)$$

$$(A, \#, \circ, ') \xrightarrow{b)} (A,+,\cdot) \xrightarrow{a)} (A, \#, \circ, ')$$

zum ursprünglichen Booleschen Ring bzw. zur ursprünglichen Booleschen Algebra zurückkommt. Mit anderen Worten: Der Übergang a) bzw. b) ist jeweils die Umkehrung von b) bzw. a).

Im Booleschen Ring und der Booleschen Algebra haben wir zwei algebraische Strukturen gefunden, die durch "Umdefinieren" auseinander hervorgehen.

§ 5 Körper, Quotientenkörper und Polynomringe über Körpern

5.1 Definition und Beispiele für Körper

5.1.1 DEFINITION:
Ein K ö r p e r ist ein kommutativer Ring, bei dem die von 0 verschiedenen Elemente bei der Multiplikation eine Gruppe bilden.

Offensichtlich ist diese Definition damit äquivalent, daß ein Körper ein kommutativer Ring mit einem Einselement $1 \neq 0$ ist, bei dem jedes von Null verschiedene Element ein inverses Element bezüglich der Multiplikation besitzt.

Beispiele für Körper: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Dies sind Körper, deren Elemente Zahlen sind; derartige Körper nennt man daher auch Zahlkörper. Diese Körper werden im VII. Kapitel von den Peanoschen Axiomen ausgehend ausführlich konstruiert.

Um weitere Beispiele für Körper zu erhalten, beweisen wir den folgenden Satz, der endliche Körper liefert.

5.1.2 SATZ:
Für $n \in \mathbb{N}_0$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis: Sei $n = p$ eine Primzahl. Dann sind

$$0 + p\mathbb{Z}\ ,\ 1 + p\mathbb{Z}\ ,\ldots,p - 1 + p\mathbb{Z}$$

genau die Elemente von $\mathbb{Z}/p\mathbb{Z}$.
Sei $0 < k < p$, $k \in \mathbb{N}$, dann sind k und p teilerfremd. Folglich gibt es $a,b \in \mathbb{N}$ mit

$$ka + pb = 1 \quad ,$$

also $ka = 1 - pb$.

Dann folgt

$$(k + p\mathbb{Z})(a + p\mathbb{Z}) = ka + p\mathbb{Z}$$

$$= 1 - pb + p\mathbb{Z} = 1 + p\mathbb{Z} \quad ,$$

also besitzt $k + p\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ das inverse Element $a + p\mathbb{Z}$. Folglich ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.
Sei jetzt $n \in \mathbb{N}_o$ keine Primzahl, dann zeigen wir, daß $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist.
1. Fall: $n = 0$, also $0\mathbb{Z} = \{0\}$. Dann gilt

$$2 + \{0\} \neq \{0\}$$

und aus der Annahme

$$(2 + \{0\})(a + \{0\}) = 2a + \{0\} = 1 + \{0\}$$

würde $2a = 1$ mit $a \in \mathbb{Z}$ folgen. Widerspruch!
2. Fall: $n = 1$, also $1\mathbb{Z} = \mathbb{Z}$. Dann besitzt der Ring $\mathbb{Z}/\mathbb{Z}$ nur ein Element, d.h. nur das Nullelement, und ist folglich kein Körper.
3. Fall: $n = ab$ mit $a, b \in \mathbb{N} \setminus \{1\}$. Dann gilt $a + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, aber $(a + n\mathbb{Z})(b + n\mathbb{Z}) = n + n\mathbb{Z} = n\mathbb{Z} = 0 + n\mathbb{Z}$.
Angenommen $a + n\mathbb{Z}$ hätte ein inverses Element $c + n\mathbb{Z}$, so folgt einerseits

$$((c + n\mathbb{Z})(a + n\mathbb{Z}))(b + n\mathbb{Z}) = (1 + n\mathbb{Z})(b + n\mathbb{Z}) = b + n\mathbb{Z}$$

und andererseits

$$(c + n\mathbb{Z})((a + n\mathbb{Z})(b + n\mathbb{Z})) = (c + n\mathbb{Z})(0 + n\mathbb{Z}) = 0 + n\mathbb{Z}$$

also $b \in n\mathbb{Z}$. Wegen b/n ergibt dies $b = 0$ oder $b = n$. Wegen $0 \neq n = ab$, $a \neq 1$, ist beides nicht möglich, also besitzt $a + n\mathbb{Z}$ kein inverses Element, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist kein Körper. //

5.2 Der Quotientenkörper eines nullteilerfreien kommutativen Ringes

Ähnlich wie in 2.9.2 wollen wir hier zu einem nullteilerfreien kommutativen Ring R inverse Elemente (bzgl. der Multiplikation) hinzufügen, um einen Körper zu erhalten, den Quotientenkörper $Q(R)$ von R.

Sei R ein nullteilerfreier kommutativer Ring.
Auf $R \times (R \setminus \{0\})$ ist durch

$$(m,n) \sim (r,s) :\Longleftrightarrow ms = nr$$

eine Äquivalenzrelation definiert.
Reflexivität: $mn = nm \Longrightarrow (m,n) \sim (m,n)$.
Symmetrie: $(m,n) \sim (r,s) \Longrightarrow ms = nr \Longrightarrow rn = sm \Longrightarrow (r,s) \sim (m,n)$.
Transitivität: $(m,n) \sim (r,s) \wedge (r,s) \sim (u,v) \Longrightarrow ms = nr \wedge rv = su \Longrightarrow (mv)s = (ms)v = nrv = n(su) = (nu)s$.
Wegen der Nullteilerfreiheit und $s \in R \setminus \{0\}$ gilt $mv = nu \Longrightarrow (m,n) \sim (u,v)$.

Sei $Q(R) := (R \times (R \setminus \{0\}))/\sim$ die Menge der Äquivalenzklassen dieser Äquivalenzrelation. Die Äquivalenzklasse von (m,n) bezeichnen wir mit $\frac{m}{n}$.

$Q(R)$ ist ein Körper mit der Addition

$$\frac{m}{n} + \frac{r}{s} := \frac{ms + nr}{ns}$$

und der Multiplikation

$$\frac{m}{n} \cdot \frac{r}{s} := \frac{mr}{ns} \quad .$$

Zunächst ist zu zeigen, daß damit Abbildungen $Q(R) \times Q(R) \longrightarrow Q(R)$ definiert werden. Dazu wenden wir III.2.3.2 an. Seien

$$\psi, \varphi: (R \times (R \setminus \{0\})) \times (R \times (R \setminus \{0\})) \longrightarrow Q(R)$$

definiert durch

$$\psi((m,n),(r,s)) := \frac{ms + nr}{ns}$$

$$\varphi((m,n),(r,s)) := \frac{mr}{ns} \quad .$$

Sei $(m,n) \sim (m',n')$ und $(r,s) \sim (r',s')$. Dann ist $mn' = nm'$ und $rs' = sr'$, also ist $(ms + nr)n's' = mn'ss' + rs'nn' = m'nss' + r'snn' = (m's' + n'r')ns$ und $mrn's' = mn'rs' = m'nr's = m'r'ns$. Damit ist

$$\frac{ms + nr}{ns} = \frac{m's' + n'r'}{n's'} \quad \text{und} \quad \frac{mr}{ns} = \frac{m'r'}{n's'} \quad ,$$

also

$$\varphi((m,n),(r,s)) = \varphi((m',n'),(r',s'))$$

und

$$\varphi((m,n),(r,s)) = \varphi((m',n'),(r',s')) \quad .$$

Nach III.2.3.2 sind damit Abbildungen

$$Q(R) \times Q(R) \ni (\frac{m}{n},\frac{r}{s}) \longmapsto \frac{ms + nr}{ns} \in Q(R)$$

$$Q(R) \times Q(R) \ni (\frac{m}{n},\frac{r}{s}) \longmapsto \frac{mr}{ns} \in Q(R)$$

definiert. Man beachte, daß mit $n,s \in R \setminus \{0\}$ auch $ns \in R \setminus \{0\}$ gilt wegen der Nullteilerfreiheit von R .

Man prüft sofort nach, daß $\frac{m}{n} = \frac{0}{1} \iff m = 0$ und daß $\frac{1}{1} = \frac{s}{s}$ für alle $s \in R \setminus \{0\}$ gelten. Mit den bekannten Regeln der Bruchrechnung zeigt man jetzt leicht, daß $(Q(R), +, \cdot)$ ein Körper ist mit $\frac{0}{1}$ als Nullelement, $\frac{1}{1}$ als Einselement und $\frac{s}{t}$ als inversem Element (bezüglich der Multiplikation) zu $\frac{t}{s}$. Man beachte dabei, daß $\frac{t}{s} \neq \frac{0}{1}$, falls $t \neq 0$.

Man hat eine injektive Abbildung $\iota : R \longrightarrow Q(R)$ mit $\iota(s) = \frac{s}{1}$. Ist nämlich $\iota(s) = \iota(t)$, also $\frac{s}{1} = \frac{t}{1}$, so ist $(s,1) \sim (t,1)$ und damit $s \cdot 1 = t \cdot 1$, daher ist $\iota : R \longrightarrow Q(R)$ injektiv. Faßt man $Q(R)$ als kommutativen Ring mit Einselement auf, so ist $\iota : R \longrightarrow Q(R)$ ein unitärer Ring-Homomorphismus, denn es ist

$$\iota(s + t) = \frac{s + t}{1} = \frac{s}{1} + \frac{t}{1} = \iota(s) + \iota(t) \quad ,$$

$$\iota(s \cdot t) = \frac{s \cdot t}{1} = \frac{s}{1} \cdot \frac{t}{1} = \iota(s) \cdot \iota(t) \quad ,$$

$$\iota(1) = \frac{1}{1} \quad .$$

Da ι injektiv ist, kann man die Elemente $s \in R$ vermöge ι mit den Elementen $\frac{s}{1} \in Q(R)$ identifizieren, also R als Teilmenge von $Q(R)$ auffassen. Dabei wirken die Addition bzw. Multiplikation von $Q(R)$ und die Addition bzw. Multiplikation von R

auf den Elementen von R in gleicher Weise, da ι ein Ringhomomorphismus ist.

5.2.1 DEFINITION:
Der oben konstruierte Körper $Q(R)$ mit dem Unterring R heißt **Quotientenkörper** von R.

5.2.2 SATZ:
Sei R ein nullteilerfreier, kommutativer Ring mit Einselement. Sei $Q(R)$ der Quotientenkörper von R mit dem oben konstruierten injektiven Ring-Homomorphismus $\iota: R \longrightarrow Q(R)$. Sei K ein weiterer Körper und $f: R \longrightarrow K$ ein injektiver Ring-Homomorphismus (wobei K als Ring aufgefaßt wird). Dann gibt es genau einen Ring-Homomorphismus (= Körper-Homomorphismus) $f': Q(R) \longrightarrow K$ mit $f'\iota = f$.

Beweis: Sei $f_1: R \times (R \setminus \{0\}) \longrightarrow K$ gegeben durch $f_1(r,s) = f(r)(f(s))^{-1}$. Dann gilt: $(r,s) \sim (x,y) \Longrightarrow ry = sx \Longrightarrow f(r)f(y) = f(s)f(x) \Longrightarrow f_1(r,s) = f(r)(f(s))^{-1} = f(x)(f(y))^{-1} = f_1(x,y)$. Dabei ist zu beachten, daß aus $s \neq 0 \neq y$ wegen der Injektivität von f folgt $f(s) \neq 0 \neq f(y)$, also sind $f(s)$ und $f(y)$ in K invertierbar. Nach III.2.3.2 induziert f_1 genau eine Abbildung $f': Q(R) \longrightarrow K$ mit $f'(\frac{r}{s}) = f(r)(f(s))^{-1}$.
f' ist ein Ring-Homomorphismus, denn es ist

$$f'(\tfrac{r}{s} + \tfrac{x}{y}) = f'(\tfrac{ry + sx}{sy})$$
$$= (f(r)f(y) + f(s)f(x))(f(s))^{-1}(f(y))^{-1}$$
$$= f(r)(f(s))^{-1} + f(x)(f(y))^{-1}$$
$$= f'(\tfrac{r}{s}) + f'(\tfrac{x}{y})$$

und

$$f'(\tfrac{r}{s}.\tfrac{x}{y}) = f'(\tfrac{rx}{sy})$$
$$= f(r)f(x)(f(s))^{-1}(f(y))^{-1}$$
$$= f'(\tfrac{r}{s})f'(\tfrac{x}{y}) \quad .$$

Für alle $r \in R$ gilt $f'\iota(r) = f'(\frac{r}{1}) = f(r)$, also

ist $f' = f$.

Ist schließlich $f'': Q(R) \longrightarrow K$ ein weiterer Ring-Homomorphismus mit $f''\iota = f$, so ist $f''(\frac{r}{s}) = f''(\frac{r}{1}(\frac{s}{1})^{-1})$ $= f''\iota(r)(f''\iota(s))^{-1} = f(r)(f(s))^{-1} = f'(\frac{r}{s})$, also ist $f' = f''$ .//

5.3 Der Polynomring mit Koeffizienten in einem Körper

Sei K ein beliebiger Körper und $K[X]$ der Polynomring in der Unbestimmten X mit Koeffizienten in K (Polynomringe siehe 3.5). Bei vielen Überlegungen in der Algebra und in anderen Gebieten der Mathematik spielt der Polynomring $K[X]$ eine wesentliche Rolle. Es sollen daher hier einige Eigenschaften von $K[X]$, die mehr oder weniger bereits aus der Schule bekannt sind, entwickelt werden.

Wir erinnern zunächst an den G r a d eines Polynoms. Gilt für $P(X) \in K[X]$

$$P(X) = p_n X^n + \ldots + p_1 X + p_o \quad , \; p_n \neq 0 \; ,$$

dann ist n der Grad des Polynoms,

$$\mathrm{Grad}(P(X)) := n \; .$$

Dem Nullpolynom, welches durch diese Definition nicht erfaßt wird, wird als Grad das Symbol $-\infty$ zugeordnet.

Insbesondere bedeutet $\mathrm{Grad}(P(X)) = 0$, daß $P(X)$ von der Form

$$P(X) = p_o \quad (= p_o X^o)$$

mit $p_o \neq 0$ ist.

5.3.1 BEMERKUNG:
Für $A(X), B(X) \in K[X]$, $A(X) \neq 0$, $B(X) \neq 0$ gilt

$$\mathrm{Grad}(A(X)B(X)) = \mathrm{Grad}(A(X)) + \mathrm{Grad}(B(X)) \; .$$

Beweis: Seien

$$A(X) = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_o \quad , \qquad a_m \neq 0 \ ,$$

$$B(X) = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_o \quad , \qquad b_n \neq 0 \ ,$$

dann folgt nach Definition der Multiplikation von Polynomen

$$A(X)B(X) = a_m b_n X^{m+n} + \text{Glieder kleineren Grades} \ .$$

Da $a_m, b_n \in K$, $a_m \neq 0$, $b_n \neq 0$, und bei einem Körper die Menge der von Null verschiedenen Elemente multiplikativ abgeschlossen ist, folgt $a_m b_n \neq 0$, also

$$\text{Grad}(A(X)B(X)) = m + n = \text{Grad}(A(X)) + \text{Grad}(B(X)) \ . \ //$$

Aus dieser Bemerkung ergibt sich insbesondere, daß das Produkt von zwei von Null verschiedenen Polynomen wieder von Null verschieden ist, d.h. $K[X]$ ist ein nullteilerfreier Ring. Daher kann im Sinne von 5.2 der Quotientenkörper konstruiert werden. Man erhält damit den sogenannten K ö r p e r der r a t i o n a l e n F u n k t i o n e n in der Unbestimmten X mit Koeffizienten in K , der meist als $K(X)$ geschrieben wird. Die Bezeichnung "Körper der rationalen Funktionen" ist insofern irreführend, als die Elemente von $K(X)$ keine Funktionen (im Sinne von Abbildungen) sind.

Bei gewissen Überlegungen hat man in einem Polynom die Unbestimmte X durch ein Element des Körpers zu ersetzen. Sei $P(X) \in K[X]$,

$$P(X) = p_n X^n + p_{n-1} X^{n-1} + \ldots + p_1 X + p_o$$

und sei $k \in K$, dann setzt man

$$P(k) := p_n k^n + p_{n-1} k^{n-1} + \ldots + p_1 k + p_o \ .$$

Folglich ist $P(k) \in K$.

5.3.2 BEMERKUNG:
Sei $k \in K$, dann wird durch

$$\Phi_k : K[X] \ni P(X) \longmapsto P(k) \in K$$

ein surjektiver Ring-Homomorphismus definiert.

Beweis: Übung für den Leser. //

Zu einem Polynom $P(X) \in K[X]$ wird oft die in folgender Weise definierte Polynomabbildung $P(x)$ betrachtet:

$$P(x): K \ni k \longmapsto P(k) \in K \ .$$

Wir wollen die zu dem Polynom $p_n X^n + \ldots + p_1 X + p_0$ gehörige Polynomabbildung mit $P(x) = p_n x^n + \ldots + p_1 x + p_0$ bezeichnen.

Man beachte, daß das Polynom $P(X)$ von der Polynomabbildung $P(x)$ wohl zu unterscheiden ist, denn verschiedene Polynome können die gleiche Polynomabbildung liefern. Sei $K = \mathbb{Z}/p\mathbb{Z}$, mit den Elementen $k_1, k_2, \ldots, k_p$, und sei

$$P(X) := \prod_{i=1}^{p} (X - k_i) \ ,$$

dann sind zwar alle Polynome $P_i(X) := P(X)^i$, $i \in \mathbb{N}$, voneinander verschieden, jedoch sind alle Polynomabbildungen $P_i(x)$, $i \in \mathbb{N}$, gleich und zwar gleich der Nullabbildung von K nach K, die jedes Element aus K auf das Nullelement von K abbildet. Der Beweis für diese Behauptung bleibt dem Leser zur Übung überlassen. Man zeige allgemeiner für zwei Polynome $A(X)$ und $B(X)$ mit Koeffizienten in $K = \mathbb{Z}/p\mathbb{Z}$:

$$A(x) = B(x) \Longleftrightarrow P(X)/A(X) - B(X) \ .$$

Zum Beweis verwende man 5.3.4. Aus 5.3.4 folgt außerdem für einen Körper mit unendlich vielen Elementen, daß zwei verschiedene Polynome verschiedene Polynomabbildungen ergeben.

Im folgenden sei K wieder ein beliebiger Körper.

5.3.3 SATZ (Euklidischer Algorithmus):
Seien $A(X), B(X) \in K[X]$ und sei $\mathrm{Grad}(B(X)) \geq 0$.
Dann existieren $P(X), Q(X) \in K[X]$ mit

$$A(X) = P(X)B(X) + Q(X) \quad \text{und} \quad \mathrm{Grad}(Q(X)) < \mathrm{Grad}(B(X)).$$

Beweis: Vollständige Induktion nach dem Grad von $A(X)$.
Induktionsbeginn: $\mathrm{Grad}(A(X)) = -\infty$, d.h. $A(X)$ sei das Nullpolynom. Wir stellen sogleich allgemeiner fest, daß die Behauptung trivialerweise für alle $A(X)$ mit $\mathrm{Grad}(A(X)) < \mathrm{Grad}(B(X))$ gilt. Dazu setze man $P(X) = 0$ und $Q(X) = A(X)$.
Induktionsschluß: Die Behauptung sei für alle Polynome von einem Grad $< m$ erfüllt. Sei $A(X)$ jetzt vom Grad m , wobei $m \geq \mathrm{Grad}(B(X))$ angenommen werden kann. Seien

$$A(X) = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_0 \quad , \quad a_m \neq 0 \ ,$$
$$B(X) = b_n X^n + b_{n-1} X^{n-1} + \ldots + b_0 \quad , \quad b_n \neq 0 \ ,$$

dann betrachten wir

$$\begin{aligned} A_1(X) &:= A(X) - a_m b_n^{-1} X^{m-n} B(X) \\ &= a_m X^m + a_{m-1} X^{m-1} + \ldots + a_0 \\ &\quad - a_m b_n^{-1} X^{m-n} (b_n X^n + b_{n-1} X^{n-1} + \ldots + b_0) \ . \end{aligned}$$

Darin ist offenbar der Koeffizient von X^m gleich 0 , so daß $A_1(X)$ einen Grad $\leq m-1$ besitzt. Nach Induktionsvoraussetzung existieren daher $P_1(X)$, $Q(X) \in K[X]$ mit

$$A_1(X) = P_1(X) B(X) + Q(X)$$

mit $\mathrm{Grad}(Q(X)) < \mathrm{Grad}(B(X))$. Dann folgt

$$\begin{aligned} A(X) &= a_m b_n^{-1} X^{m-n} B(X) + A_1(X) \\ &= (a_m b_n^{-1} X^{m-n} + P_1(X)) B(X) + Q(X) \ . \end{aligned}$$

Wenn noch

$$P(X) := a_m b_n^{-1} X^{m-n} + P_1(X)$$

gesetzt wird, ist dies die Behauptung des Satzes. //

Um aus diesem Satz eine wichtige Folgerung angeben zu können, erinnern wir daran, was unter einer N u l l s t e l l e eines Polynoms zu verstehen ist. Sei $A(X) \in K[X]$, und $k \in K$, dann heißt k Nullstelle von $A(X)$, falls $A(k) = 0$ gilt.

5.3.4 FOLGERUNG:

a) Sind $k_1,\ldots,k_m$ verschiedene Nullstellen von $A(X) \in K[X]$ in K, dann gilt

$$A(X) = (X - k_1)\ldots(X - k_m)P(X)$$

mit $P(X) \in K[X]$ und

$$\mathrm{Grad}(A(X)) = m + \mathrm{Grad}(P(X)) \ .$$

b) Ein Polynom aus $K[X]$ vom Grad n hat höchstens n verschiedene Nullstellen in K.

Beweis: a) Induktion nach m.
Induktionsbeginn: $m = 1$.
Sei k Nullstelle von $A(X)$. Nach 5.3.3 gibt es eine Zerlegung

$$A(X) = (X - k)P(X) + Q(X)$$

mit $\mathrm{Grad}(Q(X)) < \mathrm{Grad}(X - k) = 1$; also muß $\mathrm{Grad}(Q(X)) = 0$ oder $Q(X) = 0$ gelten. Ferner folgt

$$0 = A(k) = (k - k)P(k) + Q(k) = Q(k) \ .$$

Danach ist $\mathrm{Grad}(Q(X)) = 0$ (d.h. $Q(X) = q_o \neq 0$) nicht möglich, so daß $Q(X) = 0$ gelten muß.
Induktionsschluß: Nach Induktionsannahme gelte bereits

$$A(X) = (X - k_1)\ldots(X - k_{m-1})P_o(X) \ .$$

Dann folgt

$$0 = A(k_m) = (k_m - k_1)\ldots(k_m - k_{m-1})P_o(k_m) \ ,$$

und somit wegen $k_m - k_i \neq 0$ für $i = 1,\ldots,m-1$

$$P_o(k_m) = 0 \ .$$

Nach Induktionsbeginn gilt

$$P_o(X) = (X - k_m)P(X) \ ,$$

also insgesamt

$$A(X) = (X - k_1)\ldots(X - k_m)P(X) \ .$$

Die Behauptung über den Grad folgt aus 5.3.1.
b) Nach a) gilt

$$m = \mathrm{Grad}(A(X)) - \mathrm{Grad}(P(X)) \leq \mathrm{Grad}(A(X)) \ .//$$

§ 6 Moduln

6.1 Einleitung

In den Moduln lernen wir einen neuen Typ von algebraischen Strukturen kennen. Die bisher behandelten algebraischen Strukturen bestanden aus einer Menge mit einer (z.B. bei Gruppen) oder zwei Operationen (z.B. bei Ringen). Bei den Moduln werden zwei algebraische Strukturen, eine additive abelsche Gruppe und ein Ring, zu einer neuen Struktur verbunden.
Spezielle Moduln sind die linearen Vektorräume, deren Theorie zu den allgemeinen Grundlagen der Mathematik zu rechnen ist. Da die Theorie der linearen Vektorräume in den Vorlesungen für Studienanfänger in Mathematik ausführlich dargestellt wird, wollen wir uns hier auf zwei Eigenschaften von linearen Vektorräumen beschränken, die in der Theorie der Moduln wichtige und interessante Verallgemeinerungen gefunden haben. Dabei wird insbesondere die Existenz einer Basis für einen beliebigen von Null verschiedenen Vektorraum bewiesen. Dieser Beweis wird in den Anfängervorlesungen der Mathematik (aus verständlichen Gründen) manchmal übergangen und ist daher hier von Interesse. Darüber hinaus stellt er ein gutes Anwendungsbeispiel für das Zornsche Lemma dar, womit der Leser eine transfinite Schlußweise kennenlernt.

6.2 Definition und Beispiele

6.2.1 DEFINITION:
a) Ein R-Linksmodul ist ein (geordnetes) Tripel (M,R,γ) mit folgenden Eigenschaften:
   (I) M ist eine additive abelsche Gruppe.
   (II) R ist ein Ring.

(III) γ ist eine Abbildung:

$$\gamma\colon R \times M \ni (r,m) \longmapsto rm \in M$$

mit

1) Assoziativem Gesetz:

$$\forall\, r_1,r_2 \in R \;\; \forall m \in M \;\left[r_1(r_2m) = (r_1r_2)m\right]$$

2) Distributiven Gesetzen:

$$\forall\, r_1,r_2,r \in R \;\; \forall\, m_1,m_2,m \in M$$
$$\left[(r_1 + r_2)m = r_1m + r_2m \wedge r(m_1 + m_2) = rm_1 + rm_2\right]$$

(IV) (M,R,γ) heißt **unitärer R-Links-modul**, wenn R ein Ring mit Einselement 1 ist und für alle $m \in M$ gilt:

$$1m = m \;.$$

b) Ein **linearer K-Linksvektorraum** ist ein unitärer K-Linksmodul (V,K,γ), wobei K ein Körper ist.

c) Entsprechende Definitionen gelten für (unitäre) R-Rechtsmoduln und lineare K-Rechtsvektorräume.

Ist (M,R,γ) ein R-Linksmodul, dann schreibt man dafür auch kurz ${}_RM$ oder auch nur M, wenn feststeht, um welchen Ring R es sich handelt. Ist entsprechend ${}_KV$ ein linearer K-Linksvektorraum, so bezeichnet man diesen auch kurz als K-Vektorraum oder auch nur als Vektorraum, wenn feststeht, um welchen Körper K es sich handelt.

Bei einem Modul ${}_RM$ mit einem kommutativen Ring R, insbesondere also bei einem Vektorraum, ist die Unterscheidung nach der Seite, auf der R "operiert", unwesentlich und wird daher oft unterdrückt.
Ist nämlich R ein kommutativer Ring und (M,R,γ) ein R-Linksmodul, so erhält man durch die Definition

$$\gamma'\colon M \times R \ni (m,r) \longmapsto rm \in M \;,$$

d.h. also durch die Festsetzung

$$\gamma'(m,r) := \gamma(r,m)$$

einen R-Rechtsmodul, für den mit der üblichen Schreibweise $rm = \gamma(r,m)$, $mr = \gamma'(m,r)$ gilt:

$$mr = rm \quad , \quad r \in R \ , \quad m \in M \ .$$

Die Kommutativität von R wird benutzt, um für γ' das assoziative Gesetz nachzuweisen:

$$(mr_1)r_2 = r_2(r_1m) = (r_2r_1)m = (r_1r_2)m = m(r_1r_2) \ .$$

In diesem Sinne ist es gleichgültig, ob man M als R-Links- oder R-Rechtsmodul auffaßt.

6.2.2 FOLGERUNG:
Sei ${}_RM$ ein R-Linksmodul und bezeichne 0_R bzw. 0_M das Nullelement von R bzw. von M .

(1) Für alle $m \in M$ gilt $0_Rm = 0_M$;
für alle $r \in R$ gilt $r0_M = 0_M$.

(2) Für alle $m \in M$ und $r \in R$ gilt
$(-r)m = r(-m) = -(rm)$.

Beweis: (1) $0_Rm = (0_R + 0_R)m = 0_Rm + 0_Rm \implies$
$0_M = 0_Rm - 0_Rm = (0_Rm + 0_Rm) - (0_Rm) = 0_Rm + (0_Rm - (0_Rm))$
$= 0_Rm + 0_M = 0_Rm$; analog im zweiten Fall .
(2) $rm + (-r)m = (r + (-r))m = 0_Rm = 0_M \implies (-r)m = -(rm)$;
analog zeigt man $r(-m) = -(rm)$. //

Im folgenden werden die Nullelemente von M und R nicht mehr durch Indizes unterschieden, sondern beide durch 0 bezeichnet.

6.2.3 BEISPIELE:

1) Ist R ein Ring (mit Einselement), dann ist ${}_RR$ bzw. R_R ein (unitärer) R-Links- bzw. R-Rechtsmodul. Dabei ist für rm bzw. mr mit $r,m \in R$ die Multiplikation im Ring zu nehmen.
2) Ist C ein Links- bzw. Rechtsideal eines Ringes R , dann ist ${}_RC$ bzw. C_R ein R-Links- bzw. R-Rechtsmodul, wobei ebenfalls für rc bzw. cr die Multiplikation in R zu nehmen ist.
3) Ist R ein Ring, dann ist die Menge

$$R^n = \{(r_1,\ldots,r_n) \mid r_i \in R\}$$

mit der Addition

$$(r_1,\ldots,r_n) + (s_1,\ldots,s_n) := (r_1 + s_1,\ldots,r_n + s_n)$$

und der "Modulmultiplikation"

$$r(r_1,\ldots,r_n) := (rr_1,\ldots,rr_n)$$

ein R-Linksmodul.

6.3 Freie Moduln

6.3.1 DEFINITIONEN:

Sei ${}_RM$ ein R-Linksmodul.

(1) Eine Teilmenge A von M heißt **Erzeugendensystem** von M, wenn zu jedem Element $m \in M$ endlich viele Elemente $a_1,\ldots,a_l \in A$ und $r_1,\ldots,r_l \in R$ mit

$$m = \sum_{i=1}^{l} r_i a_i$$

existieren.
Sprechweise: m ist **Linearkombination** von Elementen aus A.

(2) Eine Teilmenge C von M heißt **linear unabhängig**, wenn für beliebige Elemente $c_1,\ldots,c_l \in C$ mit $c_i \neq c_j$ für $i \neq j$ und $r_1,\ldots,r_l \in R$ aus

$$0 = \sum_{i=1}^{l} r_i c_i$$

stets $r_1 = r_2 = \ldots = r_l = 0$ folgt.
Sprechweise: Die 0 läßt sich nur als triviale Linearkombination von Elementen aus C darstellen.

(3) Eine Teilmenge von M heißt **linear abhängig**, wenn sie nicht linear unabhängig ist.

(4) Eine Teilmenge B von M heißt **Basis** von M, wenn B eine linear unabhängige Erzeugendenmenge ist.

(5) Ein Modul M heißt **freier Modul**,

(ausführlich: freier R-Linksmodul), wenn eine Basis von M existiert.

6.3.2 FOLGERUNG((Eindeutigkeit der Basisdarstellung): Eine Erzeugendenmenge B von ${}_RM$ ist genau dann eine Basis, wenn für beliebige Elemente $b_1,\ldots,b_l \in B$ mit $b_i \neq b_j$ für $i \neq j$ und Elemente $r_1,\ldots,r_l$, $r'_1,\ldots,r'_l \in R$ aus

$$\sum_{i=1}^{l} r_i b_i = \sum_{i=1}^{l} r'_i b_i$$

stets $r_i = r'_i$ für alle $i = 1,\ldots,l$ folgt.

Beweis: Sei zunächst B eine Basis. Aus

$$\sum_{i=1}^{l} r_i b_i = \sum_{i=1}^{l} r'_i b_i$$

folgt

$$\sum_{i=1}^{l} (r_i - r'_i) b_i = 0 \ .$$

Da B als Basis linear unabhängig ist, impliziert diese Gleichung

$$r_i - r'_i = 0 \ , \quad i = 1,\ldots,l \ ,$$

was zu zeigen war.
Sei umgekehrt die angegebene Bedingung erfüllt und sei

$$\sum_{i=1}^{l} r_i b_i = 0 \ ;$$

da auch

$$\sum_{i=1}^{l} 0 b_i = 0$$

ist, folgt (mit $r'_i = 0$ für $i = 1,\ldots,l$) $r_i = 0$ für $i = 1,\ldots,l$, was zu zeigen war. //

Sei jetzt B eine Basis, dann kann nach Voraussetzung jedes Element $m \in M$ in der Form

$$m = \sum_{i=1}^{l} r_i b_i \ , \qquad r_i \in R$$

geschrieben werden (wobei l im allgemeinen von m abhängt!). Ohne Einschränkung kann und soll im

folgenden in dieser Linearkombination $b_i \neq b_j$ für $i \neq j$ angenommen werden, da man nach dem distributiven Gesetz mehrere Summanden mit gleichem Element aus B zusammenfassen kann. Die Linearkombination

$$m = \sum_{i=1}^{l} r_i b_i$$

wird dann als Basisdarstellung von m bezeichnet. Diese ist im Sinne von 6.3.2 eindeutig. Man beachte jedoch, daß man in der Basisdarstellung Summanden der Form $0b_i$ weglassen kann (bei der Basisdarstellung der 0 allerdings nur bis auf mindestens einen) bzw. endlich viele Summanden der Form $0b$ mit $b \in B$ hinzufügen kann.

Besitzt ${}_RM$ eine endliche Basis B etwa mit n Elementen

$$B = \{b_1, \ldots, b_n\} ,$$

dann kann in der Basisdarstellung eines jeden Elementes $m \in M$ stets über alle Basiselemente summiert werden:

$$m = \sum_{i=1}^{n} r_i b_i ,$$

und in dieser Darstellung sind die Koeffizienten $r_1, \ldots, r_n$ durch m (und B) eindeutig bestimmt.

Beachte: Eine unendliche Summe $\sum r_i b_i$ hat keinen Sinn und zwar auch dann nicht, wenn darin fast alle Summanden gleich 0 sind.

Wesentlich ist nun, daß jeder Vektorraum $\neq 0$ eine Basis besitzt, d.h. ein freier Modul ist. Hingegen besitzt nicht jeder Modul eine Basis. Freie Moduln können daher als eine Verallgemeinerung des Begriffes des Vektorraums betrachtet werden und haben mit den Vektorräumen gewisse weitere schöne Eigenschaften gemeinsam.

Hier soll bewiesen werden, daß jeder Vektorraum $\neq 0$ eine Basis besitzt, und daß andrerseits ${}_{\mathbb{Z}}\mathbb{Q}$ keine Basis besitzt, d.h. kein freier $\mathbb{Z}$-Modul ist. Der Beweis, daß jeder Vektorraum $\neq 0$ eine Basis besitzt, soll für spätere Zwecke sogleich etwas allgemeiner durchgeführt werden. Naturgemäß muß bei diesem Beweis ein transfinites Hilfsmittel benutzt werden und zwar verwenden wir das Zornsche Lemma (siehe III.3.5).

6.3.3 SATZ:
Sei ${}_K V$ ein Vektorraum und sei ${}_K V \neq 0$. Zu einer beliebigen linear unabhängigen Teilmenge C von ${}_K V$ und einer beliebigen Erzeugendenmenge E von ${}_K V$ existiert eine Menge $D_0 \subset E$, so daß $C \cup D_0$ eine Basis von ${}_K V$ ist.

Beweis: Sei

$$\mathfrak{D} = \{D \mid D \subset E \wedge C \cup D \text{ linear unabhängig}\}.$$

$\mathfrak{D}$ ist mit der Inklusion als Ordnungsrelation eine geordnete Menge. Um das Zornsche Lemma anwenden zu können, muß gezeigt werden, daß jede total geordnete Teilmenge von $\mathfrak{D}$ eine obere Schranke in $\mathfrak{D}$ besitzt. Sei $\mathfrak{T}$ eine total geordnete Teilmenge von $\mathfrak{D}$. Ist $\mathfrak{T}$ die leere Menge, dann ist jedes Element aus $\mathfrak{D}$ obere Schranke von $\mathfrak{T}$ also etwa $\emptyset$. Ist $\mathfrak{T} \neq \emptyset$, dann sei

$$T := \bigcup_{D \in \mathfrak{T}} D ;$$

offenbar ist dann T obere Schranke von $\mathfrak{T}$; es fragt sich nur, ob $T \in \mathfrak{D}$ gilt. Jedenfalls gilt $T \subset E$. Es bleibt festzustellen, ob $C \cup T$ linear unabhängig ist. Seien $t_1, \ldots, t_l$ verschiedene Elemente aus $C \cup T$ mit

$$0 = \sum_{i=1}^{l} k_i t_i \quad , \quad k_i \in K .$$

Seien $t_1, \ldots, t_s$ diejenigen Elemente, die nicht in C liegen. Für sie gilt $t_1, \ldots, t_s \in T$. Nach

Definition von T gibt es zu jedem t_i, $i = 1,\ldots,\gamma$ mindestens ein $D_i \in \mathfrak{T}$ mit $t_i \in D_i$. Aufgrund von III.3.2.2 kann $D_1 \subset D_2 \subset \ldots \subset D_\gamma$ angenommen werden. Dann folgt $t_1,\ldots,t_\gamma \in D_\gamma$. Da $C \cup D_\gamma$ linear unabhängig ist, folgt aus

$$\sum_{i=1}^{l} k_i t_i = 0$$

nun $k_1 = k_2 = \ldots = k_l = 0$, was zu zeigen war.
Nach dem Zorn'schen Lemma existiert also ein maximales Element D_o in $\mathfrak{T}$. Sei $B := C \cup D_o$.
Behauptung: B ist eine Basis.
Da B linear unabhängig ist, ist nur zu zeigen, daß B eine Erzeugendenmenge von ${}_K V$ ist.
Wir zeigen, daß jedes Element $0 \neq e_i \in E$ Linearkombination von Elementen $b_j \in B$ ist:

$$e_i = \sum_{j=1}^{l_i} k_{ij} b_j .$$

Für ein beliebiges $v \in V$ mit

$$v = \sum_{i=1}^{n} k_i' e_i$$

(E ist Erzeugendenmenge) ist dann nämlich

$$v = \sum_{i=1}^{n} \sum_{j=1}^{l_i} k_i' k_{ij} b_j .$$

Sei $e \in E$, $e \neq 0$. Ist $e \in D_o$, so ist $e = 1 \cdot e$ Linearkombination von Elementen aus B. Ist $e \notin D_o$, so ist $D_o \subsetneq D_o \cup \{e\} \subset E$. Da D_o maximal in $\mathfrak{T}$ ist, ist $D_o \cup \{e\} \notin \mathfrak{T}$, also ist $C \cup D_o \cup \{e\} = B \cup \{e\}$ linear abhängig. Folglich gibt es eine nicht-triviale Linearkombination

$$0 = k \cdot e + \sum_{j=1}^{l} k_j b_j$$

oder $0 = k \cdot e$, $k, k_j \in K$ und $k \neq 0$ (B ist linear unabhängig!). Wegen $e \neq 0$ kann $0 = k \cdot e$ nicht gelten, also ist

$$e = \sum_{j=1}^{l} -k^{-1} k_j b_j . \quad //$$

6.3.4 FOLGERUNG:
Jeder Vektorraum ${}_K V \neq 0$ besitzt eine Basis.

Beweis: In 6.3.3 wähle man für C die leere Teilmenge von ${}_K V$ und für E die ganze Menge ${}_K V$. //

Es ist sehr leicht, Beispiele für Moduln anzugeben, die keine Basis besitzen. Z.B. besitzt $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$ als $\mathbb{Z}$-Modul keine Basis, denn für jedes Element $z + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$n(z + n\mathbb{Z}) = nz + n\mathbb{Z} = n\mathbb{Z} = 0 + n\mathbb{Z} \quad ,$$

so daß keine linear unabhängige Teilmenge $\neq \emptyset$ existieren kann.

Weniger leicht, jedoch interessanter ist es zu zeigen, daß ${}_{\mathbb{Z}}\mathbb{Q}$, also die Menge der rationalen Zahlen betrachtet als $\mathbb{Z}$-Modul bei der natürlichen Addition und Multiplikation, keine Basis besitzt. Dazu beweisen wir sogleich etwas mehr.

6.3.5 SATZ:
Läßt man aus einer Erzeugendenmenge von ${}_{\mathbb{Z}}\mathbb{Q}$ endlich viele beliebige Elemente weg, dann ist die Restmenge immer noch eine Erzeugendenmenge von ${}_{\mathbb{Z}}\mathbb{Q}$.

Beweis: Offenbar genügt es zu zeigen, daß man aus einer Erzeugendenmenge ein beliebiges Element weglassen kann und die Restmenge eine Erzeugendenmenge ist. Sei A Erzeugendenmenge und sei $a_o \in A$. Da $\frac{1}{2} a_o \in \mathbb{Q}$, gibt es eine Darstellung der Form

(1) $$\frac{1}{2} a_o = z_o a_o + z_1 a_1 + \ldots + z_l a_l$$

mit verschiedenen $a_o, a_1, \ldots, a_l \in A$ und $z_o, z_1, \ldots, z_l \in \mathbb{Z}$. Ebenso gibt es eine Darstellung

(2) $$\frac{1}{1 - 2z_o} a_o = y_o a_o + y_1 a'_1 + \ldots + y_k a'_k$$

mit verschiedenen Elementen $a_o, a'_1, \ldots, a'_k \in A$ und $y_o, y_1, \ldots, y_k \in \mathbb{Z}$.
Aus (1) folgt

$$(1 - 2z_o) a_o = 2z_1 a_1 + \ldots + 2z_l a_l$$

und aus (2)

$$a_o = y_o(1 - 2z_o)a_o + y_1(1 - 2z_o)a_1' + \dots \quad .$$

Setzt man die erste der Gleichungen in die zweite ein, so ergibt sich

$$(3) \qquad a_o = y_o(2z_1a_1 + \dots + 2z_1a_1) + y_1(1 - 2z_o)a_1' + \dots + y_k(1 - 2z_o)a_k' \quad .$$

Damit ist a_o als Linearkombination von Elementen aus $A \setminus \{a_o\}$ dargestellt. Ist jetzt $q \in \mathbb{Q}$ mit der Darstellung

$$q = x_o a_o + x_1 a_1'' + \dots + x_m a_m''$$

mit $a_1'', \dots, a_m'' \in A \setminus \{a_o\}$ und $x_i \in \mathbb{Z}$, dann kann man darin für a_o die rechte Seite von (3) einsetzen und erhält q als Linearkombination von Elementen aus $A \setminus \{a_o\}$. Folglich ist $A \setminus \{a_o\}$ eine Erzeugendenmenge. //

6.3.6 FOLGERUNG:
$\mathbb{Z}^{\mathbb{Q}}$ besitzt keine Basis.

Beweis: Wir zeigen: Es gibt keine linear unabhängige Erzeugendenmenge. Ist A Erzeugendenmenge und $a_o \in A$, dann ist a_o Linearkombination von Elementen aus $A \setminus \{a_o\}$

$$a_o = z_1a_1 + z_2a_2 + \dots + z_na_n \quad , \qquad z_i \in \mathbb{Z} \; ;$$

folglich ist

$$0 = (-1)a_o + z_1a_1 + \dots + z_na_n$$

eine nichttriviale Linearkombination der 0 mit Elementen aus A. //

6.4 Halbeinfache Moduln

Eine weitere mögliche Verallgemeinerung der Vektorräume stellen die halbeinfachen Moduln dar. Um dies auseinanderzusetzen, brauchen wir einige neue Begriffe.

6.4.1 DEFINITION:
Sei $_RM$ ein Modul.

(1) Eine Teilmenge $U \subset {}_RM$ heißt **Untermodul** von $_RM$, wenn U bei der Addition von $_RM$ und der Multiplikation von $_RM$ mit Elementen aus R selbst wieder ein R-Linksmodul ist. Ist U Untermodul von $_RM$, dann wird $U \leq {}_RM$ geschrieben.

(2) Ein Untermodul U von $_RM$ heißt **direkter Summand** von $_RM$, wenn es einen Untermodul T von $_RM$ so gibt, daß gilt
   a) Jedes Element $m \in M$ läßt sich in der Form $m = u + t$, $u \in U$, $t \in T$ schreiben (kurz: $M = U + T$).
   b) $U \cap T = \{0\}$.

(3) Der Modul $_RM$ heißt **halbeinfach**, wenn jeder Untermodul von $_RM$ direkter Summand von $_RM$ ist.

Wir bemerken zunächst, daß $_{\mathbb{Z}}\mathbb{Z}$ nicht halbeinfach ist. Untermoduln von $_{\mathbb{Z}}\mathbb{Z}$ sind die Ideale von $\mathbb{Z}$, die nach 3.4.1 alle Hauptideale sind. Ist $n \in \mathbb{N}$, $n \neq 1$, dann ist das Ideal $n\mathbb{Z}$ kein direkter Summand von $_{\mathbb{Z}}\mathbb{Z}$, denn ist $m\mathbb{Z} \neq 0$ ein anderes Ideal von $\mathbb{Z}$, so gilt $0 \neq nm \in n\mathbb{Z} \cap m\mathbb{Z}$.

Dem Leser wird zur Übung empfohlen zu zeigen, daß auch $_{\mathbb{Z}}\mathbb{Q}$ nicht halbeinfach ist.

6.4.2 SATZ:
Jeder Vektorraum $_KV$ ist ein halbeinfacher Modul.

Beweis: Sei $U \leq {}_KV$. Ist $U = 0$, dann leistet $T := V$ das Gewünschte, wie sofort zu sehen. Ist $U = V$, dann ist $T = 0$ zu setzen.
Sei jetzt $0 \neq U \neq V$ und sei C eine Basis von U. Dann gibt es nach 6.3.3 eine Basis B von $_KV$ mit $C \subset B$. Sei T die Menge aller Linearkombinationen von Elementen aus $B \setminus C$. Dem Leser bleibt es als Übung überlassen zu bestätigen, daß jetzt

T das Gewünschte leistet.

6.5 Homomorphismen

Zu jeder Struktur gehören die strukturerhaltenden Abbildungen, die im Falle von Moduln Homomorphismen heißen und bei Vektorräumen auch lineare Abbildungen genannt werden.

6.5.1 DEFINITION:
Seien ${}_R M$ und ${}_R N$ R-Linksmoduln. Ein (M o d u l -) H o m o m o r p h i s m u s

$$\varphi: {}_R M \longrightarrow {}_R N$$

ist eine Abbildung von M nach N mit der folgenden Eigenschaft:

$$\forall m_1, m_2 \in M \, \forall r_1, r_2 \in R \; [\varphi(r_1 m_1 + r_2 m_2) = r_1 \varphi(m_1) + r_2 \varphi(m_2)] .$$

Homomorphismen von linearen Vektorräumen werden auch l i n e a r e A b b i l d u n g e n genannt.
Gilt $M = Qu(\varphi) = Zi(\varphi)$, dann heißt φ ein E n d o m o r p h i s m u s .

Wie leicht zu sehen, kann die Homomorphiebedingung äquivalent in die zwei folgenden Bedingungen zerlegt werden:

$$\forall m_1, m_2 \in M \; [\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)] \wedge$$
$$\forall m \in M \, \forall r \in R \; [\varphi(rm) = r\varphi(m)] .$$

Die Menge aller Homomorphismen von ${}_R M$ nach ${}_R N$ wird mit $Hom_R(M,N)$ bezeichnet. Durch folgende Definition wird $Hom_R(M,N)$ zu einer additiven, abelschen Gruppe. Seien $\alpha, \beta \in Hom_R(M,N)$, dann wird $\alpha + \beta: {}_R M \longrightarrow {}_R N$ durch

$$(\alpha + \beta)(m) := \alpha(m) + \beta(m) \quad , \quad m \in M$$

definiert.

Im Falle ${}_R M = {}_R N$ wird $Hom_R(M,M)$ auch mit

$\mathrm{End}({}_R M)$ bezeichnet. Zusätzlich zu der schon allgemein eingeführten Addition stellt jetzt die Hintereinanderausführung von Endomorphismen eine Multiplikation auf $\mathrm{End}({}_R M)$ dar, durch die $\mathrm{End}({}_R M)$ zu einem Ring wird, dem sogenannten **Endomorphismenring** von ${}_R M$. Im Falle eines Vektorraumes ${}_K V$ heißt $\mathrm{End}({}_K V)$ auch der Ring der linearen **Selbstabbildungen** von ${}_K V$.

Betrachten wir schließlich $\mathrm{Hom}_R(M,R)$, wobei R als R-Linksmodul ${}_R R$ auftritt. Durch die Definition

$$(\varphi r)(m) := \varphi(m) r \quad , \quad \varphi \in \mathrm{Hom}_R(M,R) \quad , \quad r \in R$$

wird, wie leicht nachzuprüfen, $\mathrm{Hom}_R(M,R)$ zu einem R-Rechtsmodul, der als der zu ${}_R M$ **duale Modul** bezeichnet wird.

In den letzten drei Beispielen $\mathrm{Hom}_R(M,N)$, $\mathrm{End}({}_R M)$ und $\mathrm{Hom}_R(M,R)$ haben wir gesehen, in welcher Weise Mengen von Homomorphismen selbst wieder eine algebraische Struktur sein können.

V. Kapitel: Metrische und topologische Räume

§ 1 Metrische Räume

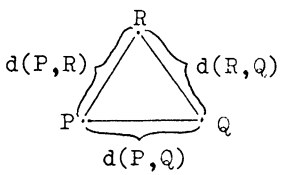
1.1 Einleitung

In der menschlichen Entwicklung entstand neben dem Bedürfnis zum Zählen sehr frühzeitig auch das Bedürfnis zum Messen von Abständen. So ist die Fähigkeit zum Messen von Abständen von Punkten in unserem dreidimensionalen physikalischen Lebensraum eine selbstverständliche Voraussetzung jeder technischen Entwicklung. Eine erste mathematische Präzisierung hat der Abstandsbegriff in der Geometrie des dreidimensionalen Anschauungsraumes gefunden. Dabei wurde zunächst nicht definiert, was unter dem Abstand $d(P,Q)$ (d für Distanz) zweier Punkte P und Q zu verstehen ist, sondern dies wurde der Anschauung entnommen, doch hat sich im Laufe der Entwicklung gezeigt, welche Eigenschaften dieses Abstandes in der Geometrie tatsächlich gebraucht werden. Es handelt sich um die folgenden Eigenschaften:

(1) Für verschiedene Punkte P und Q ist $d(P,Q)$ eine positive reelle Zahl und $d(P,P) = 0$.

(2) Symmetrie: $d(P,Q) = d(Q,P)$.

(3) Dreiecksungleichung: Für beliebige Punkte P, Q, R gilt:
$d(P,Q) \leq d(P,R) + d(R,Q)$.



Nachdem dies klar war und der Abbildungsbegriff für Mengen zur Verfügung stand, war es ein naheliegender Schritt zur Definition eines beliebigen

metrischen Raumes.

1.2 Definition und Beispiele

1.2.1 DEFINITION:
Ein Paar (M,d) heißt **metrischer Raum** mit der **Metrik** d:
(I) M ist eine Menge.
(II) d ist eine Abbildung

$$d: M \times M \longrightarrow \mathbb{R}$$

mit folgenden Eigenschaften:
(m_1) $\forall\, x,y \in M \;[d(x,y) = 0 \Longleftrightarrow x = y]$
(m_2) Symmetrie: $\forall\, x,y \in M \;[d(x,y) = d(y,x)]$
(m_3) Dreiecksungleichung:
$\forall\, x,y,z \in M \;[d(x,y) \leq d(x,z) + d(z,y)]$.
Die Elemente von M heißen **Punkte** des metrischen Raumes.

Die Eigenschaft (m_1) weicht von der zuvor angegebenen Eigenschaft (1) ab. Daß dies unwesentlich ist, zeigt die

1.2.2 FOLGERUNG:
Für einen metrischen Raum (M,d) gilt:

$$\forall\, x,y \in M \;[d(x,y) \geq 0] \;.$$

Beweis: Aufgrund von (m_1), (m_3) und (m_2) gilt
$0 = d(x,x) \leq d(x,y) + d(y,x) = 2d(x,y)$, also $d(x,y) \geq 0$.//

Die Metrik d ist demnach also eine Abbildung von $M \times M$ in die Menge der nicht-negativen reellen Zahlen, die genau die Paare (x,x) , $x \in M$ auf 0 abbildet (und die (m_2) und (m_3) erfüllt).

Zu einer Menge M kann es mehrere Metriken d geben. Ist es jedoch klar, um welche Metrik es sich handelt, so wird statt (M,d) auch nur M geschrieben und vom metrischen Raum M gesprochen.

1.2.3 BEISPIELE für metrische Räume:

1) $(\mathbb{R},d)$ mit $d(x,y) = |x-y|$.

2) $(\mathbb{R}^n,d)$, wobei gelte:
$\mathbb{R}^n = \{(x_1,\ldots,x_n) \mid x_i \in \mathbb{R}\}$
und für $x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n)$

$$d(x,y) = +\sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad .$$

d heißt die euklidische Metrik von $\mathbb{R}^n$.

3) Euklidische Metrik (V,d) (Verallgemeinerung von 1) und 2)):
Sei (V,β) ein euklidischer Raum mit dem skalaren Produkt β und der Norm $\|x\| = +\sqrt{\beta(x,x)}$, dann sei

$$d(x,y) = \|x-y\| \quad .$$

4) Weitere Metriken des $\mathbb{R}^n$:
$d_1(x,y) := \text{Max}\{|x_i - y_i| \mid i = 1,\ldots,n\}$.

$$d_2(x,y) := \sum_{i=1}^{n}|x_i - y_i| \quad .$$

5) Diskrete Metrik:
Sei M eine beliebige Menge, dann wird durch

$$d(x,y) := \begin{cases} 0 & \text{für } x = y \\ 1 & \text{für } x \neq y \end{cases}$$

die sogenannte diskrete Metrik von M definiert.
Der Leser mache sich zur Übung klar, daß im $\mathbb{R}^n$ die euklidische Metrik, die diskrete Metrik und die Metriken d_1 und d_2 alle voneinander verschieden sind.

6) $(\mathbb{N},d)$ mit

$$d(m,n) = \left|\frac{1}{m} - \frac{1}{n}\right| \quad .$$

7) Sei $\mathbb{R}^\infty := \{(x_1,x_2,x_3,\ldots) \mid x_i \in \mathbb{R}\}$ und seien $x = (x_1,x_2,x_3,\ldots)$, $y = (y_1,y_2,y_3,\ldots)$, dann wird durch

$$d(x,y) := \sum_{i=1}^{\infty}\frac{1}{2^i}\,\frac{|x_i - y_i|}{1 + |x_i - y_i|}$$

eine Metrik von $\mathbb{R}^\infty$ definiert.

8) Hilbert-Raum (H,d):

Sei $H := \{(x_1,x_2,x_3,\ldots) \mid x_i \in \mathbb{R} \wedge \text{konvergent } \sum_{i=1}^{\infty} x_i^2\}$ und sei für $x = (x_1,x_2,x_3,\ldots)$, $y = (y_1,y_2,y_3,\ldots)$ die Metrik d definiert durch

$$d(x,y) = +\sqrt{\sum_{i=1}^{\infty} (x_i - y_i)^2} \quad .$$

9) Ist (M,d) ein metrischer Raum und ist $A \subset M$, dann ist die Einschränkung von d auf $A \times A$ offensichtlich eine Metrik d_A von A. Man nennt dann (A,d_A) einen m e t r i s c h e n U n t e r r a u m von (M,d).

Der Leser beweise in allen Beispielen, daß es sich tatsächlich um Metriken handelt!

1.3 Offene Mengen in einem metrischen Raum

Offene (und abgeschlossene) Intervalle der "Zahlengeraden" sind bereits aus der Schule bekannt. Der Begriff des offenen Intervalls soll jetzt verallgemeinert werden.

1.3.1 DEFINITION:
Sei (M,d) ein metrischer Raum.

1) Seien $x_0 \in M$, $\varrho \in \mathbb{R}$, $\varrho > 0$, dann heißt

$$K(x_0,\varrho) := \{x \mid x \in M \wedge d(x_0,x) < \varrho\}$$

bzw.

$$\overline{K(x_0,\varrho)} := \{x \mid x \in M \wedge d(x_0,x) \leq \varrho\}$$

o f f e n e bzw. a b g e s c h l o s s e n e K u g e l mit dem M i t t e l p u n k t x_0 und dem R a d i u s ϱ.

2) $T \subset M$ heißt o f f e n e M e n g e von $M :\Longleftrightarrow$ $\forall\, y \in T\ \exists \varrho \in \mathbb{R}\ [\varrho > 0 \wedge K(y,\varrho) \subset T]$.

3) $A \subset M$ heißt a b g e s c h l o s s e n e M e n g e von $M :\Longleftrightarrow M \setminus A$ ist offene Menge von M.

Danach ist also eine Teilmenge T von M offen,

wenn zu jedem Punkt $y \in T$ eine offene Kugel mit y als Mittelpunkt in T enthalten ist. Gilt $K(y,\varrho) \subset T$, dann gilt selbstverständlich auch $K(y,\varepsilon) \subset T$ für jedes $\varepsilon \in \mathbb{R}$ mit $0 < \varepsilon \leq \varrho$, d.h. die offene Kugel, die noch ganz in T liegt, ist in keiner Weise eindeutig bestimmt.

Zunächst bemerken wir, daß jedes offene Intervall in $\mathbb{R}$ - wie üblich mit (a,b) bezeichnet (nicht mit dem Paar (a,b) verwechseln!) - eine offene Kugel im metrischen Raum $(\mathbb{R},d)$ mit $d(x,y) = |x-y|$ ist; für $a < b$ gilt nämlich

$$(a,b) = K\left(\frac{a+b}{2}, \frac{b-a}{2}\right) .$$

1.3.2 FOLGERUNG:
Sei (M,d) ein metrischer Raum. Dann gilt
1) Jede offene Kugel ist eine offene Menge von M.
2) Jede abgeschlossene Kugel ist eine abgeschlossene Menge von M.
3) Genau dann ist eine Teilmenge $A \subset M$ offen, wenn sie Vereinigungsmenge von offenen Kugeln ist.

Beweis: 1) Sei $y \in K(x_0,\varrho)$, dann gilt

$$K(y,\varrho - d(x_0,y)) \subset K(x_0,\varrho) ,$$

denn für $z \in K(y,\varrho - d(x_0,y))$ folgt

$$d(x_0,z) \leq d(x_0,y) + d(y,z) < d(x_0,y) + \varrho - d(x_0,y) = \varrho .$$

2) Übung für den Leser.
3) Ist A offen, so ist die Bedingung nach Definition der offenen Mengen klar, denn jeder Punkt von A liegt dann in einer in A enthaltenen offenen Kugel. Ist umgekehrt die Bedingung erfüllt, dann liegt jeder Punkt x von A in einer in A enthaltenen offenen Kugel K. Nach 1) liegt x daher auch als Mittelpunkt in einer in K enthaltenen offenen Kugel. Damit ist A offen. //

Offene bzw. abgeschlossene Kugeln im $\mathbb{R}^3$ bei der euklidischen Metrik entsprechen unserer anschaulichen Vorstellung von Kugeln. Hingegen sind offene

Kugeln eines diskreten metrischen Raumes M entweder gleich ganz M (für $\varrho > 1$) oder bestehen nur aus dem Mittelpunkt (für $\varrho \leq 1$). Der Leser mache sich die geometrische Gestalt der Kugeln im Falle der Metriken d_1 und d_2 im Beispiel 4) für $n = 2$ klar.

Wie sofort zu sehen, ist jede Teilmenge eines diskreten metrischen Raumes offen. Hingegen ist in $\mathbb{R}^n$ bei der euklidischen Metrik keine endliche Teilmenge $\neq \emptyset$ offen.

In jedem metrischen Raum (M,d) sind die Mengen $\emptyset$ und M beide sowohl offen als auch abgeschlossen.

Nach diesen erläuternden Bemerkungen betrachten wir jetzt die Menge $\mathcal{T}$ aller offenen Mengen eines metrischen Raumes (M,d) :

$$\mathcal{T} = \{T \mid T \in P(M) \wedge \text{offen } T\} .$$

1.3.3 EIGENSCHAFTEN von $\mathcal{T}$:

(t_1) Für jede Teilmenge $\mathcal{U}$ von $\mathcal{T}$ gilt:

$$\bigcup_{T \in \mathcal{U}} T \in \mathcal{T}$$

(t_2) Für jede endliche Teilmenge $\mathcal{U}$ von $\mathcal{T}$ gilt

$$\bigcap_{T \in \mathcal{U}} T \in \mathcal{T}$$

(t_3) $M \in \mathcal{T}$.

Beweis: (t_1) Nach 1.3.2 3) ist jedes $T \in \mathcal{U}$ Vereinigung von offenen Kugeln, also auch $\bigcup_{T \in \mathcal{U}} T$.

(t_2) Sei $\mathcal{U} = \{T_1, \ldots, T_n\}$ und sei

$$y \in \bigcap_{i=1}^{n} T_i ,$$

dann gibt es zu jedem T_i ein $\varrho_i \in \mathbb{R}$, $\varrho_i > 0$ mit

$$K(y, \varrho_i) \subset T_i , \quad i = 1, \ldots, n .$$

Sei $\varrho := \text{Min}\{\varrho_1, \ldots, \varrho_n\}$, dann folgt $\varrho > 0$ sowie

$$K(y, \varrho) \subset \bigcap_{i=1}^{n} T_i ,$$

was zu zeigen war.
(t_3) Nach Definition der offenen Mengen ist M offen. //

Wir bemerken zu (t_2), daß es genügt zu verlangen, daß mit $T_1, T_2 \in \mathcal{T}$ auch $T_1 \cap T_2 \in \mathcal{T}$, denn ($t_2$) folgt daraus durch Induktion. In (t_1) ist enthalten

$$\bigcup_{T \in \emptyset} T = \emptyset \in \mathcal{T} \ .$$

Hingegen ist $\bigcap_{T \in \emptyset} T$ nicht definiert.

Betrachtet man per Definition in (t_2) die leere Menge $\emptyset$ auch als endliche Teilmenge und definiert man ferner

$$\bigcap_{T \in \emptyset} T := M \ ,$$

dann kann (t_3) wegfallen. Von dieser Möglichkeit wird manchmal in der Literatur Gebrauch gemacht.

In der Untersuchung der metrischen Räume hat sich gezeigt, daß bei gewissen Überlegungen die Metrik d selbst nicht benutzt werden muß, sondern daß es genügt, auf die angegebenen Eigenschaften der Menge $\mathcal{T}$ zurückzugreifen. Dies legt es nahe zu ignorieren, daß man die Menge $\mathcal{T}$ mit Hilfe einer Metrik gewonnen hat.

Sei M jetzt eine beliebige Menge und sei $\mathcal{T} \subset P(M)$ (= Potenzmenge von M) mit den Eigenschaften (t_1), (t_2),(t_3), dann heißt das Paar $(M,\mathcal{T})$ ein topologischer Raum. Dann gilt alles, was man für metrische Räume nur unter Verwendung von (t_1), (t_2) und (t_3) hergeleitet hat, auch für topologische Räume. Darüber hinaus sieht man sofort, daß topologische Räume existieren, die nicht durch eine Metrik definiert werden können. Damit erhebt sich sogleich die interessante Frage nach einer Kennzeichnung der"metrisierbaren" topologischen Räume $(M,\mathcal{T})$, d.h. zu denen es eine Metrik d so gibt, daß $\mathcal{T}$ die Menge der offenen Mengen von (M,d) ist.

§ 2 Topologische Räume

2.1 Definition und Beispiele

2.1.1 DEFINITION:
Ein Paar $(M,\mathcal{T})$ heißt t o p o l o g i s c h e r R a u m mit der T o p o l o g i e $\mathcal{T}$: $\Longleftrightarrow$
(I) M ist eine Menge.
(II) $\mathcal{T}$ ist eine Teilmenge der Potenzmenge von M $(\mathcal{T} \subset P(M))$ mit folgenden Eigenschaften:
(t_1) Für jede Teilmenge $\mathcal{U}$ von $\mathcal{T}$ gilt

$$\bigcup_{T \in \mathcal{U}} T \in \mathcal{T} .$$

(t_2) Für jede endliche Teilmenge $\mathcal{U}$ von $\mathcal{T}$ gilt:

$$\bigcap_{T \in \mathcal{U}} T \in \mathcal{T} .$$

(t_3) $M \in \mathcal{T}$.
Die Elemente aus $\mathcal{T}$ heißen die o f f e n e n Mengen der topologischen Raumes. Die Mengen $M \setminus T$ für $T \in \mathcal{T}$ heißen die a b g e s c h l o s s e n e n Mengen des topologischen Raumes. Die Elemente aus M heißen die P u n k t e des topologischen Raumes.

Wie bei den Metriken können zu einer Menge M mehrere Topologien existieren. Ist es klar, um welche Topologie es sich bei $(M,\mathcal{T})$ handelt, so wird statt $(M,\mathcal{T})$ auch nur M geschrieben und vom topologischen Raum M gesprochen.

2.1.2 BEISPIELE für topologische Räume:
1) Zu jedem metrischen Raum (M,d) gehört in der in § 1 angegebenen Weise ein topologischer Raum, der jetzt mit $(M,\mathcal{T}_d)$ bezeichnet werden soll. $\mathcal{T}_d$ wird auch als die durch die Metrik d erzeugte Topologie bezeichnet.
Man beachte, daß verschiedene Metriken von M die gleiche Topologie von M erzeugen können. Ist dies für zwei Metriken der Fall, dann nennt man sie (topologisch) ä q u i v a l e n t .

Übung für den Leser: Stelle fest, welche der in 1.3 für $\mathbb{R}^n$ angegebenen Metriken äquivalent sind.
2) Für jede Menge M ist $\mathcal{T} := P(M)$ eine Topologie, die die diskrete Topologie von M genannt wird. Z.B. ist die durch einen diskreten metrischen Raum erzeugte Topologie die diskrete Topologie. Allerdings gibt es auch nichtdiskrete Metriken, die die diskrete Topologie erzeugen. Sei z.B. $(\mathbb{R},d)$ der metrische Raum aus Beispiel 1), dann ist der metrische Unterraum $(\mathbb{Z},d_{\mathbb{Z}})$ kein diskreter metrischer Raum. Jedoch erzeugt $d_{\mathbb{Z}}$ die diskrete Topologie von $\mathbb{Z}$.
3) Für jede Menge M ist $\mathcal{T} := \{\emptyset, M\}$ eine Topologie, die die indiskrete Topologie von M genannt wird.
4) Ist M eine endliche Menge, dann erzeugt jede Metrik von M die diskrete Topologie von M .
5) Sei M eine Menge und seien $a,b \in M$. Dann sind

$$\mathcal{T} := \{\emptyset, \{a\}, M\}$$

bzw.

$$\mathcal{T} := \{\emptyset, \{a\}, \{b\}, \{a,b\}, M\}$$

Topologien von M , die für $a \neq b$ verschieden sind.
6) Zu einer beliebigen Menge erhält man durch

$$\mathcal{T} := \{\emptyset\} \cup \{T \mid T \subset M \wedge \text{endlich } M \setminus T\}$$

eine Topologie.

2.2 Basen einer Topologie

Sei zunächst (M,d) ein metrischer Raum. Nach 1.5 ist eine Teilmenge von M genau dann offen, wenn sie Vereinigungsmenge der in ihr enthaltenen offenen Kugeln ist. Diese Situation soll jetzt verallgemeinert werden.

2.2.1 DEFINITION:
Sei $(M,\mathcal{T})$ ein topologischer Raum.

Eine Teilmenge $\mathcal{B}$ von $\mathcal{T}$ heißt **Basis** der Topologie $:\Longleftrightarrow$

$$\forall T \in \mathcal{T}\ \left[T = \bigcup_{B \in \mathcal{B} \wedge B \subset T} B\right] .$$

Nach dem zuvor Gesagten ist in einem metrischen Raum (M,d)

$$\mathcal{B} := \{K(x,\varrho) \mid x \in M \wedge \varrho \in \mathbb{R},\ \varrho > 0\}$$

eine Basis der Topologie $\mathcal{T}_d$. Im gleichen Raum erhält man weitere Basen durch folgende Konstruktion. Sei $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots)$ eine Folge von positiven reellen Zahlen mit $\lim\limits_{i\to\infty} \varepsilon_i = 0$, dann ist auch

$$\mathcal{B}_1 := \{K(x,\varepsilon_i) \mid x \in M \wedge i = 1,2,3,..\}$$

eine Basis von $\mathcal{T}_d$. Der einfache Beweis bleibt dem Leser zur Übung überlassen.

2.3 Umgebungen

Der Begriff der Umgebung liefert einen weiteren Zugang zur Definition eines topologischen Raumes und spielt bei vielen Überlegungen eine wichtige Rolle. Bekannt ist der Umgebungsbegriff oft schon aus der Schulmathematik im Spezialfall von sogenannten ε- und δ-Umgebungen.

2.3.1 DEFINITION:
Sei $(M,\mathcal{T})$ ein topologischer Raum und sei $x_0 \in M$.

1) Eine Teilmenge $T \subset M$ heißt **offene Umgebung** von $x_0 :\Longleftrightarrow$

$$x_0 \in T \wedge T \in \mathcal{T} .$$

2) Eine Teilmenge $U \subset M$ heißt **Umgebung** von $x_0 :\Longleftrightarrow$ U enthält eine offene Umgebung von x_0 .

2.3.2 FOLGERUNG:
Seien $(M,\mathcal{T})$ ein topologischer Raum, $x_0 \in M$ und sei $\mathcal{U}_{x_0}$ die Menge aller Umgebungen von x_0. Dann gilt:

(1) $\mathcal{U}_{x_0} \neq \emptyset$

(2) $\forall U_1, U_2 \in \mathcal{U}_{x_0} \; [\, U_1 \cap U_2 \in \mathcal{U}_{x_0}]$

(3) $\forall U \in \mathcal{U}_{x_0} \; \forall A \subset M \; [U \subset A \Longrightarrow A \in \mathcal{U}_{x_0}]$

(4) $\emptyset \notin \mathcal{U}_{x_0}$.

Beweis: (1) Da M offen ist, folgt $M \in \mathcal{U}_{x_0}$, also $\mathcal{U}_{x_0} = \emptyset$.
(2) Seien T_1, T_2 offene Umgebungen von x_0 mit $T_1 \subset U_1$, $T_2 \subset U_2$. Dann folgt $T_1 \cap T_2 \subset U_1 \cap U_2$. Nach (t_2) ist $T_1 \cap T_2$ offen. Da auch $x_0 \in T_1 \cap T_2$ gilt, folgt $U_1 \cap U_2 \in \mathcal{U}_{x_0}$.
(3) Nach Definition der Umgebung.
(4) Klar, da $x_0 \notin \emptyset$. //

Die Eigenschaften (1) - (4) sind die definierenden Eigenschaften eines F i l t e r s in M . Man nennt daher auch $\mathcal{U}_{x_0}$ den U m g e b u n g s f i l t e r von x_0.

2.3.3 FOLGERUNG:
Sei $(M, \mathcal{T})$ ein topologischer Raum. Dann gilt: eine Teilmenge $T \subset M$ ist genau dann offen, wenn sie Umgebung eines jeden Punktes aus T ist.

Beweis: Ist T offen, dann ist die Bedingung nach Definition der Umgebung erfüllt. Erfülle jetzt T die Bedingung, dann gibt es zu jedem $y \in T$ eine offene Menge T_y mit $y \in T_y \subset T$. Es folgt

$$T = \bigcup_{y \in T} T_y \, ,$$

also ist T nach (t_1) offen. //

Die Bedingung besagt, daß für jedes $y \in T$ gilt $T \in \mathcal{U}_y$. In dieser Formulierung geht sie in den folgenden Satz ein. Dieser Satz gibt eine Kennzeichnung eines topologischen Raumes mit Hilfe von Filtern. Er zeigt, daß man topologische Räume auch durch Vorgabe der Umgebungsfilter definieren kann.

2.3.4 SATZ:
Sei M eine Menge und sei $P(P(M))$ die Potenz-

menge der Potenzmenge von M . Dann gilt:

1) Ist

$$\mathcal{U}: \quad M \ni x \longmapsto \mathcal{U}_x \in P(P(M))$$

eine Abbildung mit den folgenden Eigenschaften

(u_1) Für jedes $x \in M$ ist $\mathcal{U}_x$ ein Filter von M (siehe 2.5),

(u_2) $\forall\, x \in M\, \forall U \in \mathcal{U}_x \,[x \in U]$

(u_3) $\forall\, x \in M\, \forall U \in \mathcal{U}_x\, \exists T \in \mathcal{U}_x\, \forall y \in T \,[T \in \mathcal{U}_y]$,

dann gibt es genau eine Topologie $\mathcal{T}$ von M , so daß für jedes $x \in M$ $\mathcal{U}_x$ der Umgebungsfilter von x ist.

2) Die offenen Mengen T der Topologie $\mathcal{T}$ sind genau die Teilmengen T von M , für die gilt

$$\forall\, y \in T \,[T \in \mathcal{U}_y] .$$

Der Beweis dieses Satzes soll hier nicht ausgeführt werden, da er in seiner Schwierigkeit über das hinausgeht, was sonst in diesen "Grundbegriffen" ausgeführt worden ist. Der Satz selbst sollte jedoch zur Information angegeben werden. Der am Beweis interessierte Leser kann diesen Beweis in Lehrbüchern der Topologie nachlesen.

Als nächster Grundbegriff soll der der Umgebungsbasis eines Punktes besprochen werden.

2.3.5 DEFINITION:
Sei $(M,\mathcal{T})$ ein topologischer Raum und sei $x \in M$. $\mathcal{B}_x$ heißt eine U m g e b u n g s b a s i s von x oder F i l t e r b a s i s von $\mathcal{U}_x$:

(1) $\mathcal{B}_x \subset \mathcal{U}_x$

(2) $\forall\, U \in \mathcal{U}_x\, \exists B \in \mathcal{B}_x \;[B \subset U]$.

Beispiel: Sei (M,d) ein metrischer Raum und $(M,\mathcal{T}_d)$ der durch d erzeugte topologische Raum. Ist $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\ldots)$ eine Folge von positiven reellen Zahlen mit $\lim\limits_{i\to\infty} \varepsilon_i = 0$, dann ist für beliebiges $x \in M$

$$\mathcal{B}_x := \{K(x,\varepsilon_i) \mid i = 1,2,3,\ldots\}$$

eine Umgebungsbasis von x .
Zum Beweis sei $U \in \mathfrak{U}_x$ und T sei eine offene Umgebung von x mit $T \subset U$. Dann gibt es eine offene Kugel $K(x,\varrho) \subset T$. Sei $\varepsilon_i \leq \varrho$, so folgt

$$K(x,\varepsilon_i) \subset K(x,\varrho) \subset T \ ,$$

also ist für $B := K(x,\varepsilon_i)$ die Basisbedingung erfüllt.

Man beachte den Unterschied zwischen einer Basis der Topologie und einer Umgebungsbasis von $\mathfrak{U}_x$.

2.4 Berührungspunkte, Häufungspunkte, offener Kern und abgeschlossene Hülle

Wir geben jetzt eine Liste von Begriffen an und untersuchen deren Beziehungen untereinander.

2.4.1 DEFINITION:
Sei $(M,\mathfrak{T})$ ein topologischer Raum, und seien $x \in M$ und $U \subset M$ sowie $U' := M \setminus U$.

1) B e r ü h r u n g s p u n k t x von U :

$$\forall\, T \in \mathfrak{T}\ [x \in T \Longrightarrow T \cap U \neq \emptyset] \ .$$

$\overline{U} :=$ Menge aller Berührungspunkte von U = a b g e s c h l o s s e n e H ü l l e von U .

2) H ä u f u n g s p u n k t x von U :

$$\forall\, T \in \mathfrak{T}\ [x \in T \Longrightarrow (T \cap U) \setminus \{x\} \neq \emptyset] \ .$$

$d(U) :=$ Menge aller Häufungspunkte von U = a b g e l e i t e t e M e n g e von U .

3) I n n e r e r P u n k t x von U :

$$\exists\, T \in \mathfrak{T}\ [x \in T \wedge T \subset U] \ .$$

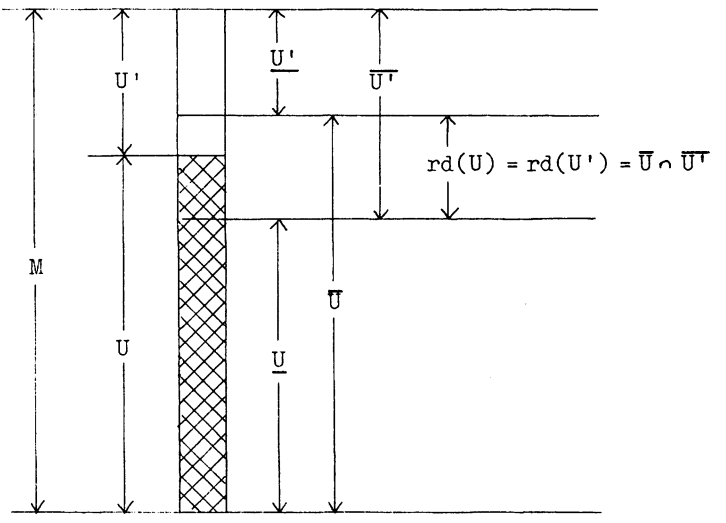
$\underline{U} :=$ Menge aller inneren Punkte von U = o f f e n e r K e r n von U .

4) R a n d p u n k t x von U :

$$\forall\, T \in \mathfrak{T}\ [x \in T \Longrightarrow (T \cap U \neq \emptyset \wedge T \cap U' \neq \emptyset)] \ .$$

$rd(U) :=$ Menge aller Randpunkte von U = R a n d von U .

Bevor wir auf Eigenschaften dieser Begriffe eingehen, geben wir in einer Skizze ihre "gegenseitige Lage" an,



Die Richtigkeit dieser Skizze ergibt sich aus dem folgenden Satz.

2.4.2 SATZ:
Sei $(M,\mathcal{T})$ ein topologischer Raum und sei $U \subset M$. Dann gilt:

(1) $\overline{U}$ ist die kleinste abgeschlossene Menge, die U enthält.

(2) $\underline{U}$ ist die größte offene Menge, die in U enthalten ist.

(3) $\overline{U} = \underline{U} \cup rd(U) \iff \underline{U} \cap rd(U) = \emptyset$

(4) $rd(U) = rd(U')$

(5) $\overline{U}' = \underline{U'}$.

Beweis: (1) Wir führen den Beweis in mehreren Schritten:

i) $U \subset \overline{U}$: Aus $x \in U$, $T \in \mathcal{T}$, $x \in T \Longrightarrow x \in T \cap U \Longrightarrow x \in \overline{U}$.

ii) $\overline{U} = \overline{\overline{U}}$: Aus $x \in \overline{U}$, $x \in T \in \mathcal{T} \Longrightarrow T \cap \overline{U} = \emptyset$, also

gibt es $y \in T \cap \overline{U}$. Wegen $y \in T \in \mathfrak{T}$, $y \in \overline{U} \Longrightarrow$ $T \cap U \neq \emptyset \Longrightarrow x \in \overline{U} \Longrightarrow \overline{U} \subset \overline{U}$. Aus $U \subset \overline{U}$ folgt andererseits $\overline{U} \subset \overline{U}$.

iii) $\overline{U}$ ist abgeschlossen: Dazu ist zu zeigen, daß $\overline{U}'$ offen ist. Sei

$$A := \bigcup_{T \in \mathfrak{T} \wedge T \subset \overline{U}'} T \ ,$$

dann ist A nach (t_1) offen. Behauptung: $A = \overline{U}'$. Angenommen, dies wäre nicht der Fall, dann sei $y \in \overline{U}' \setminus A$. Für y gilt dann

$$\forall T \in \mathfrak{T} \ [\, y \in T \Longrightarrow T \cap \overline{U} = \emptyset \,]$$

(denn $T \not\subset \overline{U}'$, da sonst $y \in A$). Daraus folgt $y \in \overline{\overline{U}} = \overline{U}$. Widerspruch!

iv) U abgeschlossen $\Longrightarrow U = \overline{U}$: Wegen $U \subset \overline{U}$ ist nur $\overline{U} \subset U$ zu zeigen. Angenommen, dies wäre nicht der Fall, dann existierte $y \in \overline{U}$, $y \notin U \Longrightarrow y \in U'$. Da U' offen und $y \in \overline{U} \Longrightarrow U' \cap U \neq \emptyset$. Widerspruch! Also gilt $\overline{U} \subset U$.

v) $\overline{U}$ ist die kleinste abgeschlossene Menge, die U enthält: Sei $U \subset A$ und A abgeschlossen $\Longrightarrow$ $\overline{U} \subset \overline{A} = A$.

(2) Sei

$$U_o := \bigcup_{T \in \mathfrak{T} \wedge T \subset U} T \ ,$$

dann ist U_o die größte offene Menge, die in U enthalten ist. Nach Definition von $\underline{U}$ gilt $\underline{U} \subset U_o$. Bleibt $U_o \subset \underline{U}$ zu zeigen. Sei $y \in U_o$, also $y \in T \in \mathfrak{T}$ mit $T \subset U \Longrightarrow y \in \underline{U} \Longrightarrow$ Behauptung.

(3) $\underline{U} \cup \mathrm{rd}(U) \subset \overline{U}$ folgt nach Definition. Sei jetzt $y \in \overline{U}$, $y \notin \underline{U} \Longrightarrow \forall T \in \mathfrak{T} \ [\, y \in T \Longrightarrow T \cap U \neq \emptyset \wedge T \not\subset U \,]$ $\Longrightarrow \forall T \in \mathfrak{T} \ [\, y \in T \Longrightarrow (T \cap U \neq \emptyset \wedge T \cap U' = \emptyset) \,] \Longrightarrow$ $y \in \mathrm{rd}(U)$. Also gilt auch $\overline{U} \subset \underline{U} \cup \mathrm{rd}(U)$.

Sei nun $y \in \underline{U} \cap \mathrm{rd}(U) \Longrightarrow \exists T \in \mathfrak{T} \ [\, y \in T \wedge T \subset U \,] \wedge$ $\forall T \in \mathfrak{T} \ [\, y \in T \Longrightarrow (T \cap U \neq \emptyset \wedge T \cap U' \neq \emptyset) \,]$. Für $T \subset U$ kann aber nicht $T \cap U' \neq \emptyset$ gelten. Widerspruch! Also folgt $\underline{U} \cap \mathrm{rd}(U) = \emptyset$.

(4) nach Definition.

(5) Wegen $U \subset \overline{U} \Longrightarrow \overline{U}' \subset U'$. Da $\overline{U}$ abgeschlossen ist, ist $\overline{U}'$ offen, also folgt $\overline{U}' \subset \underline{U'}$, denn $\underline{U'}$ ist die größte offene Menge in U' . Sei jetzt $y \in \underline{U'}$, dann gibt es $T \in \mathcal{T}$ mit $y \in T$, $T \subset U' \Longrightarrow$ $U'' = U \subset T' \Longrightarrow \overline{U} \subset T'$, da T' abgeschlossen ist $\Longrightarrow T'' = T \subset \overline{U}' \Longrightarrow y \in \overline{U}'$, also gilt auch $\underline{U'} \subset \overline{U}'$ .//

Da alle Aussagen dieses Satzes an Stelle von U auch für U' gelten, ist mit diesem Satz die anfangs angegebene Skizze gerechtfertigt. Damit sind sogleich die in 2.2.1 angegebenen Grundbegriffe erläutert - bis auf den Begriff des Häufungspunktes. Dieser spielt bei Begriffen der Analysis eine grundlegende Rolle und wird daher in Vorlesungen der Analysis eingehend diskutiert, so daß hier nicht weiter darauf eingegangen werden soll.

Wir erwähnen noch, daß man mit Hilfe von Umgebungen die sogenannten Trennungsaxiome formuliert. Als wichtigstes Beispiel geben wir den Hausdorff-Raum an.

2.4.3 DEFINITION:
Ein topologischer Raum $(M,\mathcal{T})$ heißt H a u s d o r f f - R a u m : $\Longleftrightarrow$
$\forall\, x,y \in M\,,\ x \neq y\ \exists\, T_1, T_2 \in \mathcal{T}\ \left[x \in T_1 \wedge y \in T_2 \wedge T_1 \cap T_2 = \emptyset \right]$.

Der Leser mache sich klar, daß jeder metrische Raum ein Hausdorff-Raum ist.

§ 3 Stetige Abbildungen topologischer Räume

3.1 Einleitung

Die strukturerhaltenden Abbildungen topologischer Räume heißen stetige Abbildungen. Während bei algebraischen Strukturen wie z.B. Gruppen oder Ringen unmittelbar klar ist, was eine strukturerhaltende Abbildung ist - nämlich eine solche, die mit den Operationen vertauschbar ist - liegt dies bei topologischen Räumen nicht unmittelbar auf der Hand. Vergißt man einmal die stetigen Abbildungen der Analysis, durch die die richtige Definition nahegelegt wird, so bietet sich zunächst der folgende (falsche) Ansatz an: Seien $(L,\mathfrak{S})$ und $(M,\mathfrak{T})$ topologische Räume und sei $f: L \longrightarrow M$ eine Abbildung, für die gilt $\forall S \in \mathfrak{S} \left[f_p(S) \in \mathfrak{T} \right]$, (wobei $f_p(S) = \{ f(s) \mid s \in S \}$) d.h. f erhalte offene Mengen. Daß solche Abbildungen aber keine wesentliche Rolle spielen, zeigen Beispiele. Eine Orientierung am klassischen Stetigkeitsbegriff für reelle Funktionen zeigt, daß man stattdessen $\forall T \in \mathfrak{T} \left[f^p(T) \in \mathfrak{S} \right]$ verlangen muß (wobei $f^p(T) = \{ s \mid s \in L \wedge f(s) \in T \}$ ist),d.h. daß die Urbildmengen von offenen Mengen wieder offen sein sollen.

3.2 Definition und Folgerungen

3.2.1 SATZ:
Seien $(L,\mathfrak{S})$ und $(M,\mathfrak{T})$ topologische Räume. Für eine Abbildung $f: L \longrightarrow M$ sind dann äquivalent:

(1) $\forall T \in \mathfrak{T} \left[f^p(T) \in \mathfrak{S} \right]$

(2) $\forall A \in M \left[\text{abgeschlossen } A \text{ in } M \Longrightarrow \text{abgeschlossen } f^p(A) \text{ in } L \right]$

(3) $\forall C \in L \left[f_p(\overline{C}) \subset \overline{f_p(C)} \right]$

(4) $\forall x \in L \, \forall U \in \mathcal{U}_{f(x)} \, [f^p(U) \in \mathcal{U}_x]$
(dabei sei $\mathcal{U}_{f(x)}$ bzw. $\mathcal{U}_x$ der Umgebungsfilter von $f(x)$ in M bzw. von x in L).

Beweis: (1) $\Longrightarrow$ (4): Sei $U \in \mathcal{U}_{f(x)}$ und sei $T \in \mathcal{T}$ mit $f(x) \in T \subset U$, dann ist nach (1) $f^p(T)$ offen und es gilt $x \in f^p(T) \subset f^p(U)$, also $f^p(U) \in \mathcal{U}_x$.

(4) $\Longrightarrow$ (3): Sei $z \in \overline{C}$ und sei $T \in \mathcal{T}$ mit $f(z) \in T$. Wegen (4) gibt es $S \in \mathcal{S}$ mit $z \in S \subset f^p(T)$, also folgt $S \cap C \neq \emptyset$. Es gibt folglich ein $c \in C$ mit $f(c) \in T \Longrightarrow T \cap f_p(C) \neq \emptyset \Longrightarrow f(z) \in \overline{f_p(C)}$.

(3) $\Longrightarrow$ (2): Sei $A \subset M$ abgeschlossen, dann folgt wegen (3)

$$f_p(\overline{f^p(A)}) \subset \overline{f_p(f^p(A))} \subset \overline{A} = A \Longrightarrow$$

$$\overline{f^p(A)} \subset f^p(A) \Longrightarrow$$

$$\overline{f^p(A)} = f^p(A),$$

also ist $f^p(A)$ abgeschlossen.

(2) $\Longrightarrow$ (1): Sei $T \in \mathcal{T}$, dann ist nach (2) $f^p(M \setminus T)$ abgeschlossen, also $L \setminus f^p(M \setminus T) = f^p(T)$ offen. //

3.2.2 DEFINITION:
Seien $(L,\mathcal{S})$ und $(M,\mathcal{T})$ topologische Räume und sei $f: L \longrightarrow M$ eine Abbildung.
1) f heißt s t e t i g, wenn die Bedingungen von 3.2.1 erfüllt sind. Ist f stetig, dann wird auch $f: (L,\mathcal{S}) \longrightarrow (M,\mathcal{T})$ geschrieben.
2) Sei $x \in L$. f heißt i m P u n k t x s t e t i g $:\Longleftrightarrow \forall U \in \mathcal{U}_{f(x)} \, [f^p(U) \in \mathcal{U}_x]$.

Satz 3.2.1 (4) zeigt, daß eine Abbildung $f: L \longrightarrow M$ genau dann stetig ist, wenn sie in jedem Punkt x von L stetig ist.

Wir geben jetzt eine Reihe von Folgerungen an.

3.2.3 FOLGERUNG:
Aus $g: (M_1,\mathcal{T}_1) \longrightarrow (M_2,\mathcal{T}_2)$ und $f: (M_2,\mathcal{T}_2) \longrightarrow (M_3,\mathcal{T}_3)$ folgt $fg: (M_1,\mathcal{T}_1) \longrightarrow (M_3,\mathcal{T}_3)$.

Beweis: $T \in \mathcal{T}_3 \Longrightarrow f^p(T) \in \mathcal{T}_2 \Longrightarrow g^p(f^p(T)) = (fg)^p(T) \in \mathcal{T}_1$. //

3.2.4 FOLGERUNG:
Gegeben seien topologische Räume $(L,\mathcal{T})$, $(L,\mathcal{T}_1)$, $(M,\mathcal{T}_0)$, $(M,\mathcal{T})$ mit $\mathcal{T} \subset \mathcal{T}_1$ und $\mathcal{T}_0 \subset \mathcal{T}$. Aus $f: (L,\mathcal{T}) \longrightarrow (M,\mathcal{T})$ folgt $f: (L,\mathcal{T}_1) \longrightarrow (M,\mathcal{T}_0)$.

Beweis: $T_0 \in \mathcal{T}_0 \subset \mathcal{T} \Longrightarrow f^p(T_0) \in \mathcal{T} \subset \mathcal{T}_1$. //

3.2.5 FOLGERUNG:
$1_M: (M,\mathcal{T}) \longrightarrow (M,\mathcal{T}_0) \Longleftrightarrow \mathcal{T}_0 \subset \mathcal{T}$
(d.h. die identische Abbildung von M ist dann und nur dann stetig, wenn $\mathcal{T}_0 \subset \mathcal{T}$) .

Beweis klar. //

3.2.6 FOLGERUNG:
Seien $(L,\mathcal{T})$, $(M,\mathcal{T})$ topologische Räume, $\mathcal{B}$ Basis von $\mathcal{T}$ und $f: L \longrightarrow M$. Dann gilt:
Stetig $f \Longleftrightarrow \forall B \in \mathcal{B} \left[f^p(B) \in \mathcal{T} \right]$.

Beweis: $\Longrightarrow$: klar.
$\Longleftarrow$: Sei $T \subset \mathcal{T} \Longrightarrow T = \bigcup_{B \in \mathcal{B} \wedge B \subset T} B \Longrightarrow f^p(T) = \bigcup_{B \in \mathcal{B} \wedge B \subset T} f^p(B) \subset \mathcal{T}$. //

Diese Bedingung besagt, daß man die Stetigkeitsbedingung nur für die Elemente einer Basis von $\mathcal{T}$ prüfen muß. Daher ist es erwünscht, möglichst "kleine" Basen zu haben.

Wenden wir uns jetzt der Betrachtung von Abbildungen zu, die an einer Stelle stetig sind. Wir wollen zeigen, wie die in der Analysis benutzte Definition der Stetigkeit mit der hier eingeführten Definition zusammenhängt.

3.2.7 FOLGERUNG:
Seien $(L,\mathcal{T})$, $(M,\mathcal{T})$ topologische Räume und $f: L \longrightarrow M$ eine Abbildung. Sei ferner $x \in L$ und sei $\mathcal{A}$ bzw. $\mathcal{B}$ eine Umgebungsbasis von $\mathcal{U}_x$ bzw.

$\mathcal{U}_{f(x)}$. Dann gilt:
f ist im Punkt x stetig $\Longleftrightarrow$
$\forall\, B \in \mathcal{B}\ \exists A \in \mathcal{A}\ [\, f_p(A) \subset B\,]$.

Beweis: $\Longrightarrow$: Nach Voraussetzung gilt $f^p(B) \in \mathcal{U}_x$.
Folglich existiert ein $A \in \mathcal{A}$ mit $A \subset f^p(B)$;
daraus folgt $f_p(A) \subset f_p(f^p(B)) \subset B$.

$\Longleftarrow$: Sei $U \in \mathcal{U}_{f(x)}$, dann gibt es $B \in \mathcal{B}$ mit $B \subset U$.
Sei $A \in \mathcal{A}$ mit $f_p(A) \subset B$, dann folgt $A \subset f^p(B) \subset f^p(U)$. Wegen $A \in \mathcal{A} \subset \mathcal{U}_x$ folgt $f^p(U) \in \mathcal{U}_x$, was zu zeigen war. //

3.2.8 FOLGERUNG:
Seien jetzt L und M metrische Räume und γ bzw. η die durch die Metriken von L bzw. M erzeugten Topologien. Die offenen Kugeln von L werden mit K^*, die von M mit K bezeichnet. Voraussetzungen sonst wie in 3.2.7. Dann gilt:
f ist im Punkt x stetig : $\Longleftrightarrow$
$\forall \varepsilon \in \mathbb{R}, \varepsilon > 0\ \exists \delta \in \mathbb{R}, \delta > 0\ \left[f_p(K^*(x,\delta)) \subset K(f(x),\varepsilon) \right]$.

Beweis: Man nehme in 3.2.7 die folgenden Umgebungsbasen:

$$\mathcal{A} = \{ K^*(x,\delta) \mid \delta \in \mathbb{R} \wedge \delta > 0 \}$$

$$\mathcal{B} = \{ K(f(x),\varepsilon) \mid \varepsilon \in \mathbb{R} \wedge \varepsilon > 0 \} \ .$$ //

Spezialfall von 3.2.8 für $L = M = \mathbb{R}$ mit der Metrik $d(x,y) = |x - y|$:
f ist im Punkt x stetig $\Longleftrightarrow$
$\forall \varepsilon > 0\ \exists \delta > 0\ \forall y \in \mathbb{R}\ \left[|x - y| < \delta \longrightarrow |f(x) - f(y)| < \varepsilon \right]$.

Dies zeigt, daß man in der Analysis zwei ganz spezielle, allerdings sehr zweckmäßige Umgebungsbasen benutzt.

3.3 Homöomorphismen

3.3.1 DEFINITION:
Seien (L,γ) und (M,η) topologische Räume. Ein

Homöomorphismus h von $(L,\mathcal{S})$ nach $(M,\mathcal{T})$ ist eine Bijektion $h: L \longrightarrow M$, wobei h und h^{-1} stetig sind.
Gibt es einen Homöomorphismus von $(L,\mathcal{S})$ nach $(M,\mathcal{T})$, dann heißen $(L,\mathcal{S})$ und $(M,\mathcal{T})$ homöomorph, in Zeichen $(L,\mathcal{S}) \cong (M,\mathcal{T})$ oder auch nur $L \cong M$.

Aus dieser Definition ergeben sich sofort eine Reihe von einfachen Folgerungen, deren Beweise dem Leser zur Übung überlassen bleiben.

(1) $(M,\mathcal{T}) \cong (M,\mathcal{T})$, denn $1_M: M \longrightarrow M$ ist ein Homöomorphismus.

(2) $(L,\mathcal{S}) \cong (M,\mathcal{T}) \Longrightarrow (M,\mathcal{T}) \cong (L,\mathcal{S})$

(3) $(M_1,\mathcal{T}_1) \cong (M_2,\mathcal{T}_2) \wedge (M_2,\mathcal{T}_2) \cong (M_3,\mathcal{T}_3) \Longrightarrow (M_1,\mathcal{T}_1) \cong (M_3,\mathcal{T}_3)$.

(4) Eine bijektive Abbildung $f: L \longrightarrow M$ ist dann und nur dann ein Homöomorphismus von L nach M, wenn
$f_p: \mathcal{S} \ni S \longmapsto f_p(S) \in \mathcal{T}$
eine bijektive Abbildung ist.

3.4 Initialtopologie und Finaltopologie

Zu einer Menge M sei $\mathcal{T}op(M)$ die Menge aller Topologien von M. $\mathcal{T}op(M)$ ist dann eine Teilmenge von $P(P(M))$ und $\mathcal{T}op(M)$ ist eine geordnete Menge mit der Inklusion als Ordnungsrelation. Im Sinne dieser Ordnungsrelation sprechen wir von größeren (= feineren) und kleineren (= gröberen) Topologien von M. $\mathcal{T}op(M)$ hat das größte Element $P(M)$ und das kleinste Element $\{\emptyset,M\}$. Darüber hinaus gilt:

3.4.1 HILFSSATZ:
Sei M eine Menge.
(1) $\Omega \subset \mathcal{T}op(M) \wedge \Omega \neq \emptyset \Longrightarrow \bigcap_{\mathcal{T}\in\Omega} \mathcal{T} \in \mathcal{T}op(M)$
(in Worten: Der Durchschnitt einer nichtleeren Menge von Topologien von M ist eine Topologie

von M.)

(2) $\Omega \subset \mathcal{T}_{vg}(M) \Longrightarrow$

$$\mathrm{Inf}(\Omega) = \begin{cases} \bigcap_{\mathcal{T}\in\Omega} \mathcal{T} & \text{für } \Omega \neq \emptyset \\ P(M) & \text{für } \Omega = \emptyset \end{cases} .$$

(Beachte: $\mathrm{Inf}(\Omega)$ ist die größte Topologie von M , die in allen $\mathcal{T}\in\Omega$ enthalten ist.)

(3) $\mathcal{T}_{vg}(M)$ ist ein vollständiger Verband (Def. siehe III.3.5.1) .

Beweis: (1) Die Bedingungen (t_1), (t_2), (t_3) sind zu prüfen.

(t_1): Sei $\mathcal{U} \subset \bigcap_{\mathcal{T}\in\Omega} \mathcal{T}$, dann gilt $\mathcal{U} \subset \mathcal{T}$ für jedes $\mathcal{T}\in\Omega$ und folglich $\bigcup_{T\in\mathcal{U}} T \in \mathcal{T}$ für jedes $\mathcal{T}\in\Omega$, also $\bigcup_{T\in\mathcal{U}} T \in \bigcap_{\mathcal{T}\in\Omega} \mathcal{T}$.

(t_2): Analog.

(t_3): Klar.

(2) Folgt aus (1) .

(3) Bei einer beliebigen geordneten Menge folgt aus der Existenz aller Infima die aller Suprema. Es gilt, wie leicht zu sehen,

$$\mathrm{Sup}(\Omega) = \mathrm{Inf}(\{\gamma \mid \gamma \in \mathcal{T}_{vg}(M) \wedge \forall\, \mathcal{T}\in\Omega\, [\mathcal{T} \subset \gamma]\}) \ . \ //$$

Sei jetzt L eine Menge und seien $((M_i,\mathcal{T}_i)\mid i\in\mathcal{J})$ eine Familie von topologischen Räumen und $(f_i \mid i\in\mathcal{J})$ eine Familie von Abbildungen $f_i\colon L \longrightarrow M_i$, $i\in\mathcal{J}$. Dann wird die kleinste Topologie γ von L gesucht, so daß alle f_i , $i\in\mathcal{J}$ stetig sind. Damit f_i stetig ist, müssen nach Definition der Stetigkeit $f_i^{\,p}(T_i)$, $T_i\in\mathcal{T}_i$ in γ enthalten sein. Sei nun

$$\mathcal{E} := \{f_i^{\,p}(T_i) \mid i\in\mathcal{J} \wedge T_i\in\mathcal{T}_i\} \ ,$$

dann ist wegen 3.4.1

$$(*) \qquad \gamma := \bigcup_{\mathcal{T}\in\mathcal{T}_{vg}(L)\wedge\mathcal{E}\subset\mathcal{T}} \mathcal{T}$$

die kleinste Topologie die $\mathcal{E}$ enthält.

3.4.2 DEFINITION:
Die Topologie (*) heißt I n i t i a l t o p o l o g i e von L zu den Familien $((M_i,\mathcal{T}_i)\mid i\in\mathcal{J})$, $(f_i\mid i\in\mathcal{J})$.

Statt Initialtopologie werden auch die Bezeichnungen "induzierte Topologie" und "Kofinaltopologie" benutzt.

Beispiele:

1) Sei $(M,\mathcal{T})$ gegeben sowie $L \subset M$. Bezeichne $\iota: L \longrightarrow M$ die Inklusionsabbildung. Wir wollen die Initialtopologie zur Abbildung ι (die Familie $(f_i \mid i \in \mathcal{J})$ besteht jetzt nur aus dem einen Element ι) bestimmen, die in diesem Falle auch Spurtopologie genannt wird. Jetzt ist

$$\mathcal{E} = \{\iota^P(T) \mid T \in \mathcal{T}\},$$

wobei $\iota^P(T) = T \cap L$ gilt. Wie sofort zu sehen, ist jetzt $\mathcal{E}$ bereits selbst eine Topologie, so daß jetzt $\mathcal{S} = \mathcal{E}$ folgt. Der topologische Raum $(L,\mathcal{S})$ heißt Unterraum von $(M,\mathcal{T})$.

2) Produkttopologie: Zur Familie $((M_i,\mathcal{T}_i) \mid i \in \mathcal{J})$ von topologischen Räumen sei

$$L := \prod_{i \in \mathcal{J}} M_i$$

die Produktmenge. Bezeichne $p_j: L \longrightarrow M_j$, $j \in \mathcal{J}$ die j-te Projektion von L nach M_j, die durch $p_j((x_i)) := x_j$ (x_j = j-te Komponente von (x_i)) definiert ist. Unter der Produkttopologie $\mathcal{S}$ von L versteht man dann die Initialtopologie zu den Familien

$$((M_i,\mathcal{T}_i) \mid i \in \mathcal{J}),\ (p_i \mid i \in \mathcal{J}).$$

Der topologische Raum $(L,\mathcal{S})$ heißt das topologische Produkt der Familie $((M_i,\mathcal{T}_i) \mid i \in \mathcal{J})$.

Die"duale" Konstruktion führt zum Begriff der Finaltopologie. Sei jetzt $((L_i,\mathcal{S}_i) \mid i \in \mathcal{J})$ eine Familie von topologischen Räumen und $(f_i \mid i \in \mathcal{J})$ eine Familie von Abbildungen $f_i: L_i \longrightarrow M$. Wir suchen die größte Topologie $\mathcal{T}$ von M, so daß alle f_i stetig sind. Damit f_i bei $\mathcal{T}$ stetig ist, muß für alle $T \in \mathcal{T}$ gelten: $f_i^P(T) \in \mathcal{S}_i$. Wir

haben daher jetzt die Menge

$$(*) \qquad \mathfrak{T} := \{T \mid T \subset M \wedge \forall i \in \mathfrak{J} \; [f_i^p(T) \in \mathfrak{O}_i]\}$$

zu betrachten. Wie man sofort verifizieren kann, ist $\mathfrak{T}$ selbst bereits eine Topologie von M und dann nach Definition selbstverständlich die größte derartige Topologie.

3.4.3 DEFINITION:
Die Topologie (*) heißt die F i n a l t o p o l o g i e von M zu den Familien

$$((L_i, \mathfrak{O}_i) \mid i \in \mathfrak{J}) \;, \quad (f_i \mid i \in \mathfrak{J}) \;.$$

Beispiel: Sei $(L,\mathfrak{O})$ ein topologischer Raum, sei $L \subset M$ und sei $\iota : L \longrightarrow M$ die Inklusionsabbildung. Dann gilt für die zugehörige Finaltopologie

$$\mathfrak{T} = \{S \cup U \mid S \in \mathfrak{O} \wedge U \subset M \setminus L\} \;,$$

denn $\iota^p(S \cup U) = S$ und gilt $\iota^p(T) = S \in \mathfrak{O}$ für $T \subset M$, dann ist T von der Form $T = S \cup U$ mit $U \subset M \setminus L$.

VI: Kapitel: Kategorien und Funktoren

§ 1 Einleitung

An verschiedenen Stellen wurde schon auf die Bedeutung der strukturerhaltenden Abbildungen hingewiesen. Sie sind ein wichtiges Hilfsmittel zum Studium mathematischer Objekte mit vorgegebener Struktur. Die Methoden, die dabei verwendet werden, sind häufig unabhängig von der zugrundeliegenden Struktur der untersuchten mathematischen Objekte, lassen sich also leicht auch bei anderen Strukturen einsetzen. Vielfach weist die Bemerkung "Der Beweis verläuft ähnlich oder analog" auf diese Tatsache hin. Ein Beispiel mag dies erläutern.

Der Ring mit Einselement $\mathbb{Z}$ der ganzen Zahlen hat die bemerkenswerte Eigenschaft, daß für jeden Ring mit Einselement T genau ein unitärer Ringhomomorphismus $f: \mathbb{Z} \longrightarrow T$ existiert. Das sieht man leicht ein, wenn man bedenkt, daß $f(1) = 1 \in T$ sein muß, also $f(n) = n \cdot f(1) = n \cdot 1 \in T$ für alle $n \in \mathbb{Z}$ sein muß. Wir beweisen nun den folgenden Satz:

"Sei R ein Ring mit Einselement mit der Eigenschaft, daß für jeden Ring mit Einselement T genau ein unitärer Ringhomomorphismus $f: R \longrightarrow T$ existiert, und sei S ein Ring mit Einselement mit derselben Eigenschaft, so gibt es genau einen unitären Ringhomomorphismus $g: R \longrightarrow S$ und dieser ist ein Ringisomorphismus."

Danach sind also alle Ringe mit Einselement mit der genannten Eigenschaft isomorph zu $\mathbb{Z}$.

Zum Beweis des Satzes seien $g: R \longrightarrow S$ bzw. $h: S \longrightarrow R$ die eindeutig bestimmten unitären Ring-

homomorphismen von R bzw. S aus, die nach Voraussetzung existieren. Weiter seien $hg: R \longrightarrow R$ und $gh: S \longrightarrow S$ die entsprechenden verknüpften Abbildungen. Da auch $id_R: R \longrightarrow R$ bzw. $id_S: S \longrightarrow S$ unitäre Ringhomomorphismen sind und nach Voraussetzung genau ein unitärer Ringhomomorphismus von R nach R bzw. von S nach S existiert, gilt $hg = id_R$ und $gh = id_S$. Damit ist g ein Ringisomorphismus.

Für topologische Räume gilt nun der folgende Satz:

"Sei X ein topologischer Raum mit der Eigenschaft, daß für jeden topologischen Raum Z genau eine stetige Abbildung $f: X \longrightarrow Z$ existiert, und sei Y ein topologischer Raum mit derselben Eigenschaft, so gibt es genau eine stetige Abbildung $g: X \longrightarrow Y$ und diese ist ein Homöomorphismus."

Der Beweis für diesen Satz verläuft analog zu dem oben geführten Beweis, indem man nur überall "Ring mit Einselement" durch "topologischer Raum" und "unitärer Ringhomomorphismus" durch "stetige Abbildung" ersetzt.

Nebenbei bemerkt gibt es auch einen topologischen Raum X, der die Voraussetzungen des obigen Satzes erfüllt, nämlich der leere topologische Raum $X = \emptyset$. Aufgrund des Satzes ist das (bis auf Homöomorphie) der einzige topologische Raum, der die Voraussetzung erfüllt.

Zur Formulierung der Sätze und Beweise wurde nur wenig verwendet, nämlich

a) mathematische Objekte (einer festgelegten Struktur, wie topologische Räume oder Ringe mit Einselement),
b) strukturerhaltende Abbildungen zwischen mathematischen Objekten,
c) die Tatsache, daß die Hintereinanderausführung

(Verknüpfung) von strukturerhaltenden Abbildungen wieder eine solche strukturerhaltende Abbildung ist,

d) die Tatsache, daß die identische Abbildung $id_X: X \longrightarrow X$ stets eine strukturerhaltende Abbildung ist.

Eine weitere Eigenschaft der strukturerhaltenden Abbildungen, die auch häufig verwendet wird, ist

e) die Tatsache, daß für strukturerhaltende Abbildungen $f: W \longrightarrow X$, $g: X \longrightarrow Y$, $h: Y \longrightarrow Z$ gilt

$$(hg)f = h(gf) .$$

(Dies gilt für beliebige Abbildungen, siehe III.1.5.2.)

Erstaunlich viele Sätze und Beweise lassen sich nun nur unter Zuhilfenahme der Punkte a) bis e) beweisen. Unsere anfangs angegebenen Sätze bilden ein Beispiel dafür. Deshalb faßt man a) bis e) als Axiome für einen neuen mathematischen Begriff, den der Kategorie auf.

§ 2 Kategorien

2.1 Definition und Beispiele

Man möchte alle mathematischen Objekte einer festgelegten Struktur zu einem Ganzen zusammenfassen. Das ist möglich, führt aber im allgemeinen nicht mehr zu einer Menge, sondern zu einer Klasse (vgl. die Bemerkungen über den Klassenbegriff in II.1.6.). Man kann sich eine Klasse als eine möglicherweise "sehr große Menge" vorstellen, mit der man allerdings nicht mehr uneingeschränkt alle mengentheoretischen Operationen durchführen darf. In geeigneter Weise ist aber die Definition von Abbildungen und Relationen möglich. Für uns wird diese Einschränkung keine weiteren Probleme aufwerfen. Daher werden wir den Begriff der Klasse auch nicht weiter untersuchen und axiomatisieren.

2.1.1 DEFINITION:
$\mathcal{C}$ bestehe aus
1) einer Klasse, die mit $\mathrm{Ob}\,\mathcal{C}$ bezeichnet wird, die O b j e k t k l a s s e genannt wird und deren Elemente $A,B,C,\ldots \in \mathrm{Ob}\,\mathcal{C}$ O b j e k t e heißen;
2) einer Menge $\mathrm{Mor}_{\mathcal{C}}(A,B)$ zu jedem Paar (A,B) von Objekten $A,B \in \mathrm{Ob}\,\mathcal{C}$, wobei die Elemente $f,g,h,\ldots \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ M o r p h i s m e n von A nach B genannt werden;
3) einer Abbildung, Produkt genannt,

$$\mathrm{Mor}_{\mathcal{C}}(A,B) \times \mathrm{Mor}_{\mathcal{C}}(B,C) \ni (f,g) \longmapsto gf \in \mathrm{Mor}_{\mathcal{C}}(A,C)$$

zu jedem Tripel (A,B,C) von Objekten $A,B,C \in \mathrm{Ob}\,\mathcal{C}$.

$\mathcal{C}$ heißt eine K a t e g o r i e, wenn $\mathcal{C}$ folgende Axiome erfüllt:
1) Für alle $A,B,C,D \in \mathrm{Ob}\,\mathcal{C}$ mit $(A,B) \neq (C,D)$ gilt

$$\mathrm{Mor}_{\mathcal{C}}(A,B) \cap \mathrm{Mor}_{\mathcal{C}}(C,D) = \emptyset .$$

2) Assoziativ-Gesetz: Für alle $A,B,C,D \in \mathrm{Ob}\,\mathcal{C}$

und alle $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$ und $h \in \mathrm{Mor}_{\mathcal{C}}(C,D)$ ist

$$h(gf) = (hg)f \ .$$

3) Existenz von Identitäten: Für jedes Objekt $A \in \mathrm{Ob}\,\mathcal{C}$ existiert ein Morphismus $1_A \in \mathrm{Mor}_{\mathcal{C}}(A,A)$, I d e n t i t ä t genannt, so daß für alle $B,C \in \mathrm{Ob}\,\mathcal{C}$ und alle $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ und $g \in \mathrm{Mor}_{\mathcal{C}}(C,A)$ gilt

$$f1_A = f \quad \text{und} \quad 1_A g = g \ .$$

In dieser Definition wird nicht mehr von mathematischen Objekten und strukturerhaltenden Abbildungen gesprochen, sondern nur von Objekten und Morphismen. Wir werden nämlich später Beispiele von Kategorien kennenlernen, in denen etwa die Morphismen keine strukturerhaltenden Abbildungen, ja überhaupt keine Abbildungen sind. Trotzdem werden wir auch für beliebige Morphismen weiterhin die "Pfeil-Schreibweise" verwenden. $f\colon A \longrightarrow B$ oder auch $A \xrightarrow{f} B$ bedeutet also, daß f ein Morphismus von A nach B ist, d.h. $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$. Man nennt in der Situation $f\colon A \longrightarrow B$ das Objekt A auch die Q u e l l e von f und das Objekt B das Z i e l von f , kurz $A = \mathrm{Qu}(f)$ und $B = \mathrm{Zi}(f)$. Da die Morphismen häufig keine Abbildungen sind, ist die Identität 1_A eines Objekts A dann auch nicht als identische Abbildung erklärbar. Daher müssen die wichtigsten Eigenschaften der Identität anders, nämlich in der oben angegebenen Form, ausgedrückt werden.

Die Identität 1_A für das Objekt A ist eindeutig bestimmt. Sind nämlich 1_A und $1'_A$ Identitäten für A , so gilt

$$1_A = 1_A 1'_A = 1'_A \ .$$

2.1.2 BEISPIELE FÜR KATEGORIEN:

1) $\mathcal{M}e$, die Kategorie der Mengen: $\mathrm{Ob}\,\mathcal{M}e$ sei die

Klasse aller Mengen. $\mathrm{Mor}_{\mathcal{Me}}(A,B)$ für zwei Mengen A und B sei die Menge aller Abbildungen von A nach B. Schließlich sei für Mengen A,B,C die Abbildung

$$\mathrm{Mor}_{\mathcal{Me}}(A,B) \times \mathrm{Mor}_{\mathcal{Me}}(B,C) \ni (f,g) \longmapsto gf \in \mathrm{Mor}_{\mathcal{Me}}(A,C)$$

dadurch definiert, daß gf die gewöhnliche Hintereinanderausführung der Abbildungen g und f sei, d.h. daß für alle $a \in A$ gelte $gf(a) = g(f(a))$.

Es müssen jetzt die drei Axiome für eine Kategorie nachgeprüft werden. Seien A,B,C,D Mengen und sei $f \in \mathrm{Mor}_{\mathcal{Me}}(A,B) \cap \mathrm{Mor}_{\mathcal{Me}}(C,D)$. Nach Definition einer Abbildung (III.1.3.1) ist f ein Tripel $(Qu(f),Zi(f),Gr(f))$ und daher gilt $A = Qu(f) = C$ bzw. $B = Zi(f) = D$, also $(A,B) = (C,D)$. Damit ist das erste Axiom erfüllt. Das zweite und dritte Axiom wurde in III.1.5.2 nachgewiesen. Die Identität ist hier die identische Abbildung.

In den folgenden Beispielen (2) bis (14) werden jeweils nur die Objekte und Morphismen einer Kategorie angegeben. Das Produkt der Morphismen ist immer die Hintereinanderausführung von Abbildungen. Dem Leser bleibt es überlassen, die Axiome für Kategorien in den nachfolgenden Beispielen zu verifizieren.

Name der Kategorie	Symbol	Objekte	Morphismen
2) Kategorie der Monoide	$\mathcal{Mo}$	Monoide	Monoidhomomorphismen
3) " der Gruppen	$\mathcal{Gr}$	Gruppen	Gruppenhomomorphismen
4) " der abelschen Gruppen	$\mathcal{Ab}$	abelsche Gruppen	Gruppenhomomorphismen
5) " der Ringe	$\mathcal{Ri}$	Ringe	Ringhomomorphismen
6) " der unitären Ringe	-	Ringe mit 1-Element	unitäre Ringhomomorphismen
7) " der Körper	-	Körper	(unitäre) Ringhomomorphismen

Name der Kategorie	Symbol	Objekte	Morphismen
8) Kategorie der unitären R-Links-Moduln	$\mathcal{R}\text{-}\mathcal{M}od$	unitäre R-Links-Moduln	(R-Modul-)Homomorphismen
9) " der K-Vektorräume	$\mathcal{K}\text{-}\mathcal{M}od$	K-Vektorräume	lineare Abbildungen
10) " der geordneten Mengen	-	geordnete Mengen	ordnungstreue Abbildungen
11) " der Booleschen Verbände	$\mathcal{B}v$	Boolesche Verbände	Boolesche Verbandshomomorphismen
12) " der unitären Booleschen Ringe	$\mathcal{B}r$	Boolesche Ringe mit 1-Element	unitäre Ringhomomorphismen
13) " der Booleschen Algebren	$\mathcal{B}a$	Boolesche Algebren	Boolesche Algebrenhomomorphismen
14) " der topologischen Räume	$\mathcal{T}o$	topologische Räume	stetige Abbildungen

Wir tragen an dieser Stelle die Definition von einigen in den Beispielen genannten strukturerhaltenden Abbildungen nach. Seien $(M,\leq)$ und $(N,\leq)$ zwei geordnete Mengen. Eine Abbildung $f: M \longrightarrow N$ heißt o r d n u n g s t r e u , wenn gilt

$$\forall\, m_1,m_2 \in M \left[m_1 \leq m_2 \Longrightarrow f(m_1) \leq f(m_2) \right] .$$

Sind $(M,\leq)$ und $(N,\leq)$ Verbände, so heißt $f: M \longrightarrow N$ ein V e r b a n d s h o m o m o r p h i s m u s , wenn

$$\forall\, m_1,m_2 \in M \left[f(m_1 \cap m_2) = f(m_1) \cap f(m_2) \wedge f(m_1 \cup m_2) = f(m_1) \cup f(m_2) \right] .$$

Es ist leicht zu sehen, daß ein Verbandshomomorphismus immer ordnungstreu ist. Seien $(M,\leq)$ und $(N,\leq)$ Boolesche Verbände. Ein Verbandshomomorphismus heißt ein B o o l e s c h e r V e r b a n d s h o m o m o r p h i s m u s , wenn eine der beiden folgenden äquivalenten Bedingungen erfüllt ist:

a) $\forall\, m \in M \left[f(m') = f(m)'\right]$,

b) $f(e_M) = e_N \wedge f(\sigma_M) = \sigma_N$.

Von der Äquivalenz von a) und b) kann man sich leicht überzeugen.

Seien $(A, *, \circ, ')$ und $(B, *, \circ, ')$ Boolesche Algebren. Eine Abbildung $f: A \longrightarrow B$ heißt B o o l e s c h e r A l g e b r e n h o m o m o r p h i s m u s , wenn

a) $\forall\, a,b \in A \left[f(a * b) = f(a) * f(b)\right]$

b) $\forall\, a,b \in A \left[f(a \circ b) = f(a) \circ f(b)\right]$

c) $\forall\, a \in A \left[f(a') = f(a)'\right]$.

Man kann die Bedingung c) wieder durch $f(\sigma) = \sigma$ und $f(e) = e$ ersetzen.

Wir wollen nun einige Beispiele für Kategorien angeben, in denen die Morphismen nicht als strukturerhaltende Abbildungen auftreten. Auch in diesen Beispielen soll es dem Leser überlassen bleiben, die Axiome für Kategorien zu verifizieren.

15) Kategorie der Mengenkorrespondenzen: Die Klasse der Objekte sei die Klasse aller Mengen. Die Morphismen einer Menge A in eine Menge B seien die (Korrespondenzen oder) Relationen von A in B . Es bleibt das Produkt von Relationen $f: A \longrightarrow B$ und $g: B \longrightarrow C$ zu $gf: A \longrightarrow C$ zu definieren. Dieses soll einfach die in III.1.1.4 definierte Produktrelation sein.

16) Sei $(M, \leq)$ eine geordnete Menge. Wir fassen die Menge M als Klasse von Objekten auf; die Elemente $m \in M$ sind also die Objekte unserer Kategorie $\underline{M}$. Für $m,n \in M$ definieren wir

$$\mathrm{Mor}_{\underline{M}}(m,n) := \begin{cases} \{(m,n)\} & \text{falls } m \leq n \\ \emptyset & \text{sonst .} \end{cases}$$

Für das Produkt

$$\mathrm{Mor}_{\underline{M}}(m,n) \times \mathrm{Mor}_{\underline{M}}(n,p) \longrightarrow \mathrm{Mor}_{\underline{M}}(m,p)$$

bleibt dann nur eine Möglichkeit, weil $Mor_{\underline{M}}(m,p)$ nur entweder ein oder kein Element enthält. Aufgrund der Eigenschaften einer geordneten Menge ist das Produkt immer definiert und assoziativ.

§ 3 Morphismen

3.1 Isomorphismen

3.1.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Ein Morphismus $f: A \longrightarrow B$ in $\mathcal{C}$ heißt I s o m o r p h i s m u s , wenn es einen Morphismus $g: B \longrightarrow A$ gibt, so daß gilt

$$fg = 1_B \quad \text{und} \quad gf = 1_A \ .$$

g heißt i n v e r s e r M o r p h i s m u s zu f und wird häufig mit f^{-1} bezeichnet.

3.1.2 BEHAUPTUNG:
Ein Isomorphismus f besitzt genau einen inversen Morphismus.

Beweis: Seien nämlich $g: B \longrightarrow A$ und $g': B \longrightarrow A$ inverse Morphismen zu $f: A \longrightarrow B$, d.h. gelte $fg = 1_B$, $gf = 1_A$ und $fg' = 1_B$, $g'f = 1_A$, so ist $g = g1_B = gfg' = 1_A g' = g'$. //

3.1.3 BEHAUPTUNG:
a) Ist $f: A \longrightarrow B$ ein Isomorphismus, so ist auch $f^{-1}: B \longrightarrow A$ ein Isomorphismus und es gilt $(f^{-1})^{-1} = f$.
b) Sind $f: A \longrightarrow B$ und $g: B \longrightarrow A$ Isomorphismen, so ist auch $gf: A \longrightarrow C$ ein Isomorphismus und es gilt $(gf)^{-1} = f^{-1}g^{-1}$.

Beweis: a) Wegen $f^{-1}f = 1_B$ und $ff^{-1} = 1_A$ ist f^{-1} ein Isomorphismus mit dem inversen Morphismus f . Wegen 3.1.2 ist daher $(f^{-1})^{-1} = f$.
b) Es ist $(gf)(f^{-1}g^{-1}) = g(ff^{-1})g^{-1} = g1_B g^{-1} = gg^{-1} = 1_C$ und $(f^{-1}g^{-1})(gf) = f^{-1}(g^{-1}g)f = f^{-1}1_B f = f^{-1}f = 1_A$, also ist gf ein Isomorphismus mit dem inversen Morphismus $f^{-1}g^{-1}$. Wegen 3.1.2 gilt $(gf)^{-1} = f^{-1}g^{-1}$. //

In der Kategorie $\mathcal{M}e$ der Mengen sind die Isomorphismen genau die bijektiven Abbildungen (III.1.6.1).

In den Beispielen 2) - 14) von Kategorien, in denen Morphismen strukturerhaltende Abbildungen sind, sind Isomorphismen immer bijektiv. Das folgt ebenfalls aus III.1.6.1. Jedoch sind bijektive strukturerhaltende Abbildungen nicht immer Isomorphismen, wie das folgende Beispiel zeigt.

In der Kategorie $\mathcal{T}_{\mathcal{O}}$ sind die Isomorphismen die Homöomorphismen (siehe V.3.3). Wir geben ein Beispiel für eine bijektive stetige Abbildung, die kein Homöomorphismus ist, für die also die inverse Abbildung nicht stetig ist.

Seien auf der Menge $M = \{a,b\}$ die Topologien $\mathcal{S} = \{\emptyset, \{a\}, \{b\}, M\}$ und $\mathcal{T} = \{\emptyset, M\}$ gegeben. Sei $f: M \longrightarrow M$ definiert durch $f(a) = a$, $f(b) = b$. Dann ist $f: (M,\mathcal{S}) \longrightarrow (M,\mathcal{T})$ bijektiv und stetig, da $f^P(\emptyset) = \emptyset$ und $f^P(M) = M$ offen bzgl. $\mathcal{S}$ sind. Dabei sei $f^P(B) = \{a \in M \mid f(a) \in B\}$ für $B \subset M$ das Urbild der Teilmenge B unter f . Wäre nun f ein Homöomorphismus, so wäre die Umkehrabbildung $f^{-1}: (M,\mathcal{T}) \longrightarrow (M,\mathcal{S})$ stetig. Da aber $(f^{-1})^P(\{a\}) = \{a\}$ nicht offen bzgl. $\mathcal{T}$ ist, ist f^{-1} nicht stetig. Also ist f zwar ein bijektiver Morphismus, aber kein Isomorphismus in der Kategorie $\mathcal{T}_{\mathcal{O}}$.

Für die Beispiele 2) - 9) ist es allerdings richtig, daß die Isomorphismen genau die bijektiven Morphismen der entsprechenden Kategorien sind. Davon kann sich der Leser leicht selbst überzeugen.

3.2 Monomorphismen

3.2.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Ein Morphismus $f: A \longrightarrow B$ in $\mathcal{C}$ heißt **Monomorphismus**, wenn für jedes Objekt C aus $\mathrm{Ob}\,\mathcal{C}$ und alle $g,h \in \mathrm{Mor}_{\mathcal{C}}(C,A)$ gilt $fg = fh \Longrightarrow g = h$. Man sagt auch, daß f **linkskürzbar** ist.

3.2.2 BEHAUPTUNG:
Seien $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$.
a) Sind f und g Monomorphismen, so ist gf ein Monomorphismus.
b) Ist gf ein Monomorphismus, so ist f ein Monomorphismus.

Beweis: a) Seien $h,k \in \mathrm{Mor}_{\mathcal{C}}(D,A)$. Dann gilt
$(gf)h = (gf)k \Longrightarrow g(fh) = g(fk) \Longrightarrow fh = fk \Longrightarrow h = k$.
b) $fh = fk \Longrightarrow gfh = gfk \Longrightarrow h = k$. //

3.2.3 BEHAUPTUNG:
Ist f ein Isomorphismus, so ist f ein Monomorphismus.

Beweis: $fg = fh \Longrightarrow f^{-1}fg = f^{-1}fh \Longrightarrow g = h$. //

3.2.4 BEHAUPTUNG:
$f: A \longrightarrow B$ ist genau dann ein Monomorphismus, wenn für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Abbildung

$$\mathrm{Mor}_{\mathcal{C}}(C,f): \mathrm{Mor}_{\mathcal{C}}(C,A) \ni g \longrightarrow fg \in \mathrm{Mor}_{\mathcal{C}}(C,B)$$

injektiv ist.

Beweis: Die Aussage ist eine einfache Umformulierung der Definition eines Monomorphismus. //

In den Kategorien aus den Beispielen 1) - 14) ist jede injektive strukturerhaltende Abbildung ein Monomorphismus. Sind nämlich A,B Objekte aus einer dieser Kategorien und ist $f: A \longrightarrow B$ eine injektive strukturerhaltende Abbildung, ist C ein weiteres Objekt und sind $g,h \in \mathrm{Mor}_{\mathcal{C}}(C,A)$ mit $g \neq h$, so gibt es ein Element $c \in C$ mit $g(c) \neq h(c)$. Da f injektiv ist, ist auch $fg(c) \neq fh(c)$, also $fg \neq fh$. Damit ist f ein Monomorphismus.

In den Beispielen 1) - 14) ist auch jeder Monomorphismus eine injektive strukturerhaltende Abbildung. Das ist schwieriger zu beweisen. Für die Kategorie $\mathcal{M}e$ der Mengen wurde diese Aussage in

III.1.5.3 bewiesen. Wir beweisen sie noch für die Kategorie $\mathcal{AG}$ der abelschen Gruppen.

Seien A,B abelsche Gruppen und $f: A \longrightarrow B$ ein nicht-injektiver Gruppenhomomorphismus. Seien $x,y \in A$ mit $x \neq y$ und $f(x) = f(y)$. Seien $g,h \in \mathrm{Mor}_{\mathcal{AG}}(\mathbb{Z},A)$ definiert durch $g(n) = nx$ und $h(n) = ny$. Man sieht leicht, daß g und h Gruppenhomomorphismen sind. Weiter ist $g \neq h$ wegen $g(1) = x \neq y = h(1)$. Jedoch ist $fg(n) = f(nx) = nf(x) = nf(y) = f(ny) = fh(n)$ für alle $n \in \mathbb{Z}$, also $fg = fh$. Also kann f kein Monomorphismus sein, wenn f nicht injektiv ist.

In der Kategorie der teilbaren abelschen Gruppen mit teilbaren abelschen Gruppen als Objekten und Gruppenhomomorphismen als Morphismen gibt es jedoch Monomorphismen, die nicht injektiv sind. Dabei nennen wir eine abelsche Gruppe A teilbar, wenn für jede natürliche Zahl $n \neq 0$ gilt: $nA = A$, d.h. wenn zu jedem $a \in A$ und $n \neq 0$ ein $a' \in A$ mit $na' = a$ existiert. In der Tat ist der Restklassenhomomorphismus $f: \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z}$ der rationalen Zahlen in die rationalen Zahlen modulo den ganzen Zahlen ein Monomorphismus in unserer Kategorie. Seien nämlich $g,h: A \longrightarrow \mathbb{Q}$ zwei Morphismen in dieser Kategorie mit $g \neq h$. Dann existiert ein $a \in A$ mit $g(a) - h(a) = \frac{r}{s} \neq 0$ mit $r \in \mathbb{N}$, $s \in \mathbb{Z}$. Dann existiert ein $a' \in A$ mit $2ra' = a$. Es ist $2r(g(a') - h(a')) = g(a) - h(a) = \frac{r}{s}$, also $g(a') - h(a') = \frac{1}{2s} \notin \mathbb{Z}$, d.h. $fg(a') \neq fh(a')$. Damit ist f ein Monomorphismus, der als Abbildung nicht injektiv ist.

3.3 Epimorphismen

3.3.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Ein Morphismus $f: B \longrightarrow A$ in $\mathcal{C}$ heißt **Epimorphismus**, wenn für jedes Objekt C aus $\mathrm{Ob}\,\mathcal{C}$ und alle $g,h \in \mathrm{Mor}_{\mathcal{C}}(A,C)$ gilt

$$gf = hf \Longrightarrow g = h \ .$$

Man sagt auch, daß f r e c h t s - k ü r z b a r ist.

3.3.2 BEHAUPTUNG:
Seien $f \in \mathrm{Mor}_{\mathcal{C}}(B,A)$, $g \in \mathrm{Mor}_{\mathcal{C}}(C,B)$.
a) Sind f und g Epimorphismen, so ist fg ein Epimorphismus.
b) Ist fg ein Epimorphismus, so ist f ein Epimorphismus.

Beweis: a) Seien $h,k \in \mathrm{Mor}_{\mathcal{C}}(A,D)$. Dann gilt
$h(fg) = k(fg) \Longrightarrow (hf)g = (kf)g \Longrightarrow hf = kf \Longrightarrow h = k$.
b) $hf = kf \Longrightarrow hfg = kfg \Longrightarrow h = k$. //

3.3.3 BEHAUPTUNG:
Ist f ein Isomorphismus, so ist f ein Epimorphismus.

Beweis: $gf = hf \Longrightarrow gff^{-1} = hff^{-1} \Longrightarrow g = h$. //

3.3.4 BEHAUPTUNG:
$f: B \longrightarrow A$ ist genau dann ein Epimorphismus, wenn für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Abbildung

$$\mathrm{Mor}_{\mathcal{C}}(f,C): \mathrm{Mor}_{\mathcal{C}}(A,C) \ni g \longmapsto gf \in \mathrm{Mor}_{\mathcal{C}}(B,C)$$

injektiv ist.

Beweis: Die Aussage ist eine einfache Umformulierung der Definition eines Epimorphismus. //

Der Leser wird bemerkt haben, daß die Definition und die obigen Behauptungen völlig in Analogie zu den entsprechenden Aussagen für Monomorphismen formuliert worden ist. Der einzige (wichtige!) Unterschied ist, daß alle Pfeilrichtungen der Morphismen umgekehrt worden sind. Man nennt dieses Verfahren "Dualisieren". Wir wollen im Rahmen dieser Einführung darauf jedoch nicht näher eingehen.

In den Kategorien aus den Beispielen 1) - 14) ist jede surjektive strukturerhaltende Abbildung ein

Epimorphismus. Sind nämlich A,B Objekte aus einer dieser Kategorien $\mathcal{C}$ und ist $f: B \longrightarrow A$ eine surjektive strukturerhaltende Abbildung, ist C ein weiteres Objekt und sind $g,h \in Mor_{\mathcal{C}}(A,C)$ mit $g \neq h$, so gibt es ein Element $a \in A$ mit $g(a) \neq h(a)$. Da f surjektiv ist, gibt es ein $b \in B$ mit $f(b) = a$. Also ist $gf(b) = g(a) \neq h(a) = hf(b)$ und $gf \neq hf$. Damit ist f ein Epimorphismus.

In den Kategorien aus den Beispielen 1,3,4,8,9,10 und 14 ist jeder Epimorphismus eine surjektive strukturerhaltende Abbildung.(Daher findet man in vielen Lehrbüchern Epimorphismen auch definiert als surjektive strukturerhaltende Abbildungen. Nach unserer Definition ist das jedoch nicht dasselbe, wie Beispiele noch zeigen werden.) Das ist schwieriger zu beweisen. Für die Kategorie der Mengen wurde diese Aussage in III.1.5.3 bewiesen. Wir beweisen sie noch für die Kategorien $\mathcal{Ab}$ der abelschen Gruppen und die Kategorie $\mathcal{Gr}$ der Gruppen.

3.3.5 BEHAUPTUNG:
In $\mathcal{Ab}$ ist jeder Epimorphismus surjektiv.

Beweis: Seien A,B abelsche Gruppen und sei $f: B \longrightarrow A$ ein Epimorphismus in $\mathcal{Ab}$. Sei $C = A/Bi(f)$ und $\nu : A \longrightarrow A/Bi(f)$ der natürliche Epimorphismus (IV.2.7.4). Weiter sei $g: A \longrightarrow A/Bi(f)$ die Nullabbildung, d.h. $g(A) = \overline{0} = Bi(f)$ für alle $a \in A$. Für alle $b \in B$ gilt $\nu f(b) = f(b) + Bi(f) = Bi(f) = gf(b)$, also ist $\nu f = gf$. Da f ein Epimorphismus ist, ist $\nu = g$. Es ist $Ker(g) = A$ und $Ker(\nu) = Bi(f)$, also $A = Ker(g) = Ker(\nu) = Bi(f)$. Damit ist f surjektiv.//

3.3.6 BEHAUPTUNG:
In $\mathcal{Gr}$ ist jeder Epimorphismus surjektiv.

Beweis: Sei $f: B \longrightarrow A$ ein Epimorphismus in $\mathcal{Gr}$.

Sei $C := f(B)$ das Bild von f. Wir wollen zeigen, daß $C = A$ ist. Dann ist f surjektiv.
Zunächst konstruieren wir eine Gruppe S als "Testobjekt" und geeignete Homomorphismen $h,k: A \longrightarrow S$. Dazu betrachten wir $A/C = \{aC \mid a \in A\}$, die Menge der Rechtsnebenklassen. Wir benötigen ein weiteres Element, das nicht in A/C enthalten ist und das wir mit ∞ bezeichnen wollen, also $\infty \notin A/C$. Sei nun $S := S(A/C \cup \{\infty\})$ die Gruppe der invertierbaren Abbildungen der Menge $A/C \cup \{\infty\}$ auf sich (vgl. IV.2.2.2).
Der gesuchte Homomorphismus $h: A \longrightarrow S$ sei definiert durch $h(a_1)(a_2C) = a_1a_2C$ und $h(a_1)(\infty) = \infty$. Das Element a_1a_2C ist unabhängig von der Auswahl des Repräsentanten a_2 für a_2C. Sei nämlich $a_2C = b_2C$, so ist $b_2 = a_2c$ für ein $c \in C$. Also ist $a_1b_2C = a_1a_2cC = a_1a_2C$. Weiter ist $h(a_1)$ eine invertierbare Abbildung von $A/C \cup \{\infty\}$ auf sich mit der inversen Abbildung $h(a_1^{-1})$ wegen $h(a_1^{-1})h(a_1)(a_2C) = a_1^{-1}a_1a_2C = a_2C$ und $h(a_1^{-1})h(a_1)(\infty) = \infty$, also $h(a_1^{-1})h(a_1) = id_{A/C\cup\{\infty\}}$ und entsprechend $h(a_1)h(a_1^{-1}) = id_{A/C\cup\{\infty\}}$. Damit ist $h: A \longrightarrow S$ eine wohldefinierte Abbildung. h ist sogar ein Gruppenhomomorphismus, denn es gilt $h(a_1a_2)(a_3C) = a_1a_2a_3C = h(a_1)h(a_2)(a_3C)$ und $h(a_1a_2)(\infty) = \infty = h(a_1)h(a_2)(\infty)$.
Zur Konstruktion des Gruppenhomomorphismus $k: A \longrightarrow S$ benötigen wir das Element $s \in S$ mit $s(aC) = aC$ für $a \notin C$, $s(C) = \infty$ und $s(\infty) = C$.
Wegen $s^2 = id_{A/C\cup\{\infty\}}$ ist s eine invertierbare Abbildung, also $s \in S$.
Nun definieren wir $k: A \longrightarrow S$ durch $k(a) = sh(a)s$.
Wegen $k(a_1a_2) = sh(a_1a_2)s = sh(a_1)h(a_2)s = sh(a_1)ssh(a_2)s = k(a_1)k(a_2)$ ist k ein Gruppenhomomorphismus.
Wir wollen nun zeigen, daß $hf = kf$. Sei dazu $b \in B$, $a \in A$ und $a \notin C$. Dann ist $k(f(b))(aC) = sh(f(b))s(aC) = sh(f(b))(aC) = f(b)aC$ (weil aus $a \in C$ folgt $f(b)a \in C$) $= h(f(b))(aC)$. Weiter gilt

$k(f(b))(C) = sh(f(b))s(C) = sh(f(b))(\infty) = s(\infty) = C$ und $k(f(b))(\infty) = sh(f(b))s(\infty) = sh(f(b))(C) = s(f(b)C) = s(C)$ (wegen $C = f(B)$) $= \infty$. Damit ist $hf = kf$.
Da f ein Epimorphismus ist, ist $h = k$. Ist $a \in A$, so ist $aC = h(a)(C) = k(a)(C) = sh(a)s(C) = sh(a)(\infty) = s(\infty) = C$, also $a \in C$ und folglich $A = C$. Damit ist gezeigt, daß jeder Epimorphismus in der Kategorie $\mathcal{Gr}$ der Gruppen surjektiv ist. //

Wir geben nun zwei Beispiele von Epimorphismen an, die nicht surjektiv sind. Das erste Beispiel bezieht sich auf die Kategorie $\mathcal{Mo}$ der Monoide. Die natürliche Einbettung $f: \mathbb{N}_0 \longrightarrow \mathbb{Z}$ von dem Monoid $\mathbb{N}_0$ der natürlichen Zahlen (unter der Addition) in die abelsche Gruppe $\mathbb{Z}$ der ganzen Zahlen (vgl. VII.2.2) ist ein Epimorphismus. Seien nämlich $g,h: \mathbb{Z} \longrightarrow M$ zwei Monoidhomomorphismen mit $gf = hf$. Die Monoidoperation in M sei $*$ und das neutrale Element sei e . Für $n \in \mathbb{Z}$ betrachten wir zwei Fälle. Ist $n \geq 0$, so ist $n = f(n)$, also $g(n) = gf(n) = hf(n) = h(n)$. Ist $n < 0$, so ist $g(n) * g(-n) = g(n + (-n)) = g(0) = e = h(0) = h(n + (-n)) = h(n) * h(-n) = h(n) * g(-n)$. Ebenso ist $g(-n) * g(n) = e = g(-n) * h(n)$. Wegen $g(n) = g(n) * g(-n) * h(n) = h(n)$ ist damit $g(n) = h(n)$ für alle $n \in \mathbb{Z}$, also $g = h$.

Das zweite Beispiel eines Epimorphismus, der nicht surjektiv ist, ist die natürliche Einbettung $f: \mathbb{Z} \longrightarrow \mathbb{Q}$ vom Ring der ganzen Zahlen in den Körper der rationalen Zahlen, aufgefaßt als Morphismus in der Kategorie $\mathcal{Ri}$ der Ringe. Wir brauchen nur zu zeigen, daß f ein Epimorphismus ist. Seien $g,h: \mathbb{Q} \longrightarrow A$ gegeben mit $gf = hf$. Dann ist $g(n) = h(n)$ für alle ganzen Zahlen n in $\mathbb{Q}$ und $g(1) = h(1)$. Also ist $g(n)g(\frac{1}{n}) = h(n)h(\frac{1}{n})$. Wir erhalten so, daß gilt

$g(\frac{1}{n}) = g(\frac{1}{n}\cdot n\cdot\frac{1}{n}) = g(\frac{1}{n})g(n)g(\frac{1}{n}) = g(\frac{1}{n})h(n)h(\frac{1}{n}) =$

$g(\frac{1}{n})g(n)h(\frac{1}{n}) = h(\frac{1}{n})h(n)h(\frac{1}{n}) = h(\frac{1}{n})$.

Für ein beliebiges Element $\frac{m}{n} \in \mathbb{Q}$ gilt daher

$g(\frac{m}{n}) = g(m\cdot\frac{1}{n}) = g(m)g(\frac{1}{n}) = h(m)h(\frac{1}{n}) = h(\frac{m}{n})$,

also $g = h$.

Da f bezüglich beliebiger Ringhomomorphismen rechts-kürzbar ist und sogar ein unitärer Ringhomomorphismus ist, ist f auch bezüglich unitärer Ringhomomorphismen rechts-kürzbar. Also ist $f: \mathbb{Z} \longrightarrow \mathbb{Q}$ auch in der Kategorie der Ringe mit Einselement ein Epimorphismus, der nicht surjektiv ist.

3.4 Schnitte und Retraktionen

3.4.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Ein Morphismus $f: A \longrightarrow B$ in $\mathcal{C}$ heißt ein Schnitt, wenn es einen Morphismus $g: B \longrightarrow A$ gibt, so daß gilt

$$gf = 1_A \ .$$

Ein Morphismus $f: A \longrightarrow B$ in $\mathcal{C}$ heißt eine Retraktion, wenn es einen Morphismus $g: B \longrightarrow A$ gibt, so daß gilt

$$fg = 1_B \ .$$

3.4.2 BEMERKUNG:
Sind $f: A \longrightarrow B$ und $g: B \longrightarrow A$ Morphismen in $\mathcal{C}$, so daß $gf = 1_A$ gilt. Dann sind f ein Schnitt und g eine Retraktion.
Zu jedem Schnitt können wir also eine Retraktion und zu jeder Retraktion einen Schnitt finden, jedoch sind diese im allgemeinen nicht eindeutig bestimmt.

3.4.3 BEHAUPTUNG:
$f: A \longrightarrow B$ ist genau dann ein Isomorphismus, wenn f ein Schnitt und eine Retraktion ist.

Beweis: Ist f ein Isomorphismus, so ist $f^{-1}f = 1_A$ und $ff^{-1} = 1_B$, d.h. f ist ein Schnitt und eine Retraktion. Ist umgekehrt f ein Schnitt und eine Retraktion, so gibt es Morphismen $g,h \in \mathrm{Mor}_{\mathcal{C}}(B,A)$ mit $gf = 1_A$ und $fh = 1_B$. Daraus folgt $g = g1_B = gfh = 1_B h = h$, also ist f ein Isomorphismus. //

3.4.4 BEHAUPTUNG:
a) Ist $f: A \longrightarrow B$ ein Schnitt, so ist f ein Monomorphismus.
b) Ist $f: A \longrightarrow B$ eine Retraktion, so ist f ein Epimorphismus.

Beweis: a) $fh = fk \Longrightarrow gfh = gfk \Longrightarrow 1_A h = 1_A k \Longrightarrow h = k$.
b) $hf = kf \Longrightarrow hfg = kfg \Longrightarrow h1_A = k1_A \Longrightarrow h = k$. //

3.4.5 BEHAUPTUNG:
a) Sind $f: A \longrightarrow B$ und $g: B \longrightarrow C$ Schnitte, so ist $gf: A \longrightarrow C$ ein Schnitt. Ist $gf: A \longrightarrow C$ ein Schnitt, so ist $f: A \longrightarrow B$ ein Schnitt.
b) Sind $f: B \longrightarrow A$ und $g: C \longrightarrow B$ Retraktionen, so ist $fg: C \longrightarrow A$ eine Retraktion. Ist $fg: C \longrightarrow A$ eine Retraktion, so ist $f: B \longrightarrow A$ eine Retraktion.

Beweis: a) $g'g = 1_B$ und $f'f = 1_A \Longrightarrow f'g'gf = f'1_B f = f'f = 1_A$. $h(gf) = 1_A \Longrightarrow (hg)f = 1_A$.
b) $gg' = 1_B$ und $ff' = 1_A \Longrightarrow fgg'f' = f1_B f' = ff' = 1_A$. $(fg)h = 1_A \Longrightarrow f(gh) = 1_A$. //

3.4.6 BEHAUPTUNG:
a) $f: A \longrightarrow B$ ist genau dann ein Schnitt, wenn für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Abbildung

$$\mathrm{Mor}_{\mathcal{C}}(f,C): \mathrm{Mor}_{\mathcal{C}}(B,C) \ni h \longmapsto hf \in \mathrm{Mor}_{\mathcal{C}}(A,C)$$

surjektiv ist.
b) $f: B \longrightarrow A$ ist genau dann eine Retraktion, wenn

für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Abbildung

$$\mathrm{Mor}_{\mathcal{C}}(C,f)\colon \mathrm{Mor}_{\mathcal{C}}(C,B) \ni h \longmapsto fh \in \mathrm{Mor}_{\mathcal{C}}(C,A)$$

surjektiv ist.

Beweis: a) Sei f ein Schnitt mit $gf = 1_A$. Sei $k \in \mathrm{Mor}_{\mathcal{C}}(A,C)$. Dann ist $\mathrm{Mor}_{\mathcal{C}}(f,C)(kg) = kgf = k$, also ist $\mathrm{Mor}_{\mathcal{C}}(f,C)$ surjektiv. Sei $\mathrm{Mor}_{\mathcal{C}}(f,C)$ für alle $C \in \mathrm{Ob}\,\mathcal{C}$ surjektiv, so ist insbesondere $\mathrm{Mor}_{\mathcal{C}}(f,A)$ surjektiv, also existiert ein $g \in \mathrm{Mor}_{\mathcal{C}}(B,A)$ mit $\mathrm{Mor}_{\mathcal{C}}(f,A)(g) = 1_A$. Dann ist $gf = 1_A$ und f ein Schnitt.
b) Dieser Beweis verläuft dual zu a), d.h. durch Umkehren der Pfeilrichtungen der Morphismen, und wird dem Leser überlassen. //

In den Kategorien aus den Beispielen 1 - 14 ist jeder Schnitt eine injektive strukturerhaltende Abbildung und jede Retraktion eine surjektive strukturerhaltende Abbildung. Ist nämlich $f\colon A \longrightarrow B$ ein Schnitt mit $gf = 1_A$ und ist $f(a_1) = f(a_2)$, so ist $a_1 = gf(a_1) = gf(a_2) = a_2$, also ist f injektiv. Ist $f\colon B \longrightarrow A$ eine Retraktion mit $fg = 1_A$ und sei $a \in A$. Dann ist $f(g(a)) = a$, also ist f surjektiv. Daß Schnitt (Retraktion) ein wesentlich stärkerer Begriff ist als injektive (surjektive) strukturerhaltende Abbildung, geht daraus hervor, daß in den Beispielen 2 - 6 surjektive Morphismen keine Retraktionen sind (aber z.B. in 1,7 und 9) und in den Beispielen 1 - 8 injektive Morphismen keine Schnitte sind (aber z.B. in 9). Selbst in der Kategorie $\mathcal{M}$ der Mengen ist die injektive Abbildung $f\colon \emptyset \longrightarrow \{\emptyset\}$ kein Schnitt. Allerdings sind alle injektiven Abbildungen $f\colon A \longrightarrow B$ mit $A \neq \emptyset$ Schnitte in $\mathcal{M}$.

Wir tragen noch einige weitere Bezeichnungen für Morphismen nach, werden diese speziellen Morphismen jedoch nicht weiter diskutieren. $f\colon A \longrightarrow B$ heißt B i m o r p h i s m u s , wenn f ein Monomorphismus

und ein Epimorphismus ist. $f: A \longrightarrow B$ heißt E n d o m o r p h i s m u s , wenn $A = B$ ist. $f: A \longrightarrow B$ heißt A u t o m o r p h i s m u s , wenn f ein Isomorphismus und ein Endomorphismus ist. Bimorphismen sind im allgemeinen keine Isomorphismen, wie das Beispiel der Einbettung $f: \mathbb{Z} \longrightarrow \mathbb{Q}$ in $\mathcal{R}i$ zeigt.

Übung: $f: A \longrightarrow B$ ist ein Schnitt und ein Epimorphismus genau dann, wenn f ein Isomorphismus ist. $f: B \longrightarrow A$ ist eine Retraktion und ein Monomorphismus genau dann, wenn f ein Isomorphismus ist.

§ 4 Funktoren

4.1 Definition und Beispiele

Der neu eingeführte Begriff der Kategorie definiert eine neue Art von mathematischen Objekten. Auch für diese mathematischen Objekte gibt es strukturerhaltende Abbildungen, die Funktoren genannt werden. Zahlreiche Beispiele legen es nahe, zwei verschiedene Arten von Funktoren einzuführen, die kovarianten und die kontravarianten Funktoren, die sich im Verhalten in Bezug auf die Morphismenrichtungen unterscheiden.

4.1.1 DEFINITION:
Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. $\mathcal{F}$ bestehe aus
1) einer Abbildung

$$\mathrm{Ob}\,\mathcal{C} \ni A \longmapsto \mathcal{F}(A) \in \mathrm{Ob}\,\mathcal{D} \quad *)$$

2) je einer Abbildung

$$\mathcal{F}(A,B)\colon \mathrm{Mor}_{\mathcal{C}}(A,B) \ni f \longmapsto \mathcal{F}(A,B)(f) \in \mathrm{Mor}_{\mathcal{D}}(\mathcal{F}(A),\mathcal{F}(B))$$

zu jedem Paar (A,B) von Objekten $A,B \in \mathrm{Ob}\,\mathcal{C}$.

$\mathcal{F}$ heißt ein k o v a r i a n t e r F u n k t o r , wenn $\mathcal{F}$ folgende Axiome erfüllt:
1) $\mathcal{F}(A,A)(1_A) = 1_{\mathcal{F}(A)}$ für alle $A \in \mathrm{Ob}\,\mathcal{C}$
2) $\mathcal{F}(A,C)(gf) = \mathcal{F}(B,C)(g)\mathcal{F}(A,B)(f)$
für alle $A,B,C \in \mathrm{Ob}\,\mathcal{C}$ und alle $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$.

Ein kovarianter Funktor $\mathcal{T}\colon \mathcal{C} \longrightarrow \mathcal{D}$ bildet also Objekte in Objekte ab und Morphismen in Morphismen, so daß das Produkt von Morphismen und die Identitäten respektiert werden.

4.1.2 DEFINITION:
Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. $\mathcal{F}$ bestehe aus
1) einer Abbildung

$$\mathrm{Ob}\,\mathcal{C} \ni A \longmapsto \mathcal{F}(A) \in \mathrm{Ob}\,\mathcal{D}$$

*) Siehe 2.1

2) je einer Abbildung

$$\mathcal{F}(A,B)\colon \mathrm{Mor}_{\mathcal{C}}(A,B) \ni f \longmapsto \mathcal{F}(A,B)(f) \in \mathrm{Mor}_{\mathcal{L}}(\mathcal{F}(B),\mathcal{F}(A))$$

zu jedem Paar (A,B) von Objekten $A,B \in \mathrm{Ob}\,\mathcal{C}$.

$\mathcal{F}$ heißt ein k o n t r a v a r i a n t e r F u n k t o r , wenn $\mathcal{F}$ folgende Axiome erfüllt:

1) $\mathcal{F}(A,A)(1_A) = 1_{\mathcal{F}(A)}$ für alle $A \in \mathrm{Ob}\,\mathcal{C}$

2) $\mathcal{F}(A,C)(gf) = \mathcal{F}(A,B)(f)\mathcal{F}(B,C)(g)$
für alle $A,B,C \in \mathrm{Ob}\,\mathcal{C}$ und alle $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$.

In Pfeilschreibweise bildet der kontravariante Funktor $\mathcal{F}\colon \mathcal{C} \longrightarrow \mathcal{L}$ einen Morphismus $f\colon A \longrightarrow B$ aus $\mathcal{C}$ in den Morphismus $\mathcal{F}(A,B)(f)\colon \mathcal{F}(B) \longrightarrow \mathcal{F}(A)$ ab. Die Pfeilrichtung der Morphismen wird also umgedreht. Der Leser mag sich in der Pfeilschreibweise das Axiom 2 klarmachen.

Eines der wichtigsten Beispiele für Funktoren ist schon in den Begriff der Kategorie selbst eingeschlossen. Für ein fest gewähltes Objekt $A \in \mathrm{Ob}\,\mathcal{C}$ definieren wir einen kovarianten Funktor $\mathrm{Mor}_{\mathcal{C}}(A,-)\colon \mathcal{C} \longrightarrow \mathcal{M}e$ von der Kategorie $\mathcal{C}$ in die Kategorie der Mengen. Der Funktor $\mathrm{Mor}_{\mathcal{C}}(A,-)$ muß also jedem Objekt B aus der Kategorie $\mathcal{C}$ eine Menge zuordnen und jedem Morphismus $f\colon B \longrightarrow C$ aus der Kategorie $\mathcal{C}$ eine Abbildung von Mengen. Das erreichen wir wie folgt:

$$\mathrm{Mor}_{\mathcal{C}}(A,-)(B) := \mathrm{Mor}_{\mathcal{C}}(A,B)$$

$$\mathrm{Mor}_{\mathcal{C}}(A,-)(B,C)(f) := \mathrm{Mor}_{\mathcal{C}}(A,f) .$$

Dabei sei $\mathrm{Mor}_{\mathcal{C}}(A,f)$ wie in 3.2.4 definiert, also als

$$\mathrm{Mor}_{\mathcal{C}}(A,f)\colon \mathrm{Mor}_{\mathcal{C}}(A,B) \ni g \longmapsto fg \in \mathrm{Mor}_{\mathcal{C}}(A,C) .$$

Damit ist die Abbildung auf den Objekten und Morphismen sinnvoll definiert, denn $\mathrm{Mor}_{\mathcal{C}}(A,-)(B,C)(f)$ ist tatsächlich ein Element von $\mathrm{Mor}_{\mathcal{M}e}(\mathrm{Mor}_{\mathcal{C}}(A,-)(B),\mathrm{Mor}_{\mathcal{C}}(A,-)(C))$, also eine Abbildung von $\mathrm{Mor}_{\mathcal{C}}(A,B)$ nach $\mathrm{Mor}_{\mathcal{C}}(A,C)$. Es sind

noch die Axiome für kovariante Funktoren nachzuprüfen. Für $B \in \mathrm{Ob}\,\mathcal{C}$ ist $\mathrm{Mor}_{\mathcal{C}}(A,-)(B,B)(1_B) = \mathrm{Mor}_{\mathcal{C}}(A,1_B)$. Es ist also zu zeigen

$$\mathrm{Mor}_{\mathcal{C}}(A,1_B) = \mathrm{id}_{\mathrm{Mor}_{\mathcal{C}}(A,B)} \quad .$$

Tatsächlich gilt für jedes $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ die folgende Rechnung:

$$\mathrm{Mor}_{\mathcal{C}}(A,1_B)(f) = 1_B f = f = \mathrm{id}_{\mathrm{Mor}_{\mathcal{C}}(A,B)}(f) \quad .$$

Um das zweite Axiom nachzuprüfen, seien $B,C,D \in \mathrm{Ob}\,\mathcal{C}$ und $f \in \mathrm{Mor}_{\mathcal{C}}(B,C)$, $g \in \mathrm{Mor}_{\mathcal{C}}(C,D)$ und $h \in \mathrm{Mor}_{\mathcal{C}}(A,B)$. Dann gilt

$$\begin{aligned}&\left[\mathrm{Mor}_{\mathcal{C}}(A,-)(B,D)(gf)\right](h) = \mathrm{Mor}_{\mathcal{C}}(A,gf)(h) = gfh\\ &= \mathrm{Mor}_{\mathcal{C}}(A,g)(fh) = \mathrm{Mor}_{\mathcal{C}}(A,g)\mathrm{Mor}_{\mathcal{C}}(A,f)(h)\\ &= \left[\mathrm{Mor}_{\mathcal{C}}(A,-)(C,D)(g)\mathrm{Mor}_{\mathcal{C}}(A,-)(B,C)(f)\right](h) \quad ,\end{aligned}$$

also ist

$$\mathrm{Mor}_{\mathcal{C}}(A,-)(B,C)(gf) = \mathrm{Mor}_{\mathcal{C}}(A,-)(C,D)(g)\mathrm{Mor}_{\mathcal{C}}(A,-)(B,C)(f) \quad .$$

Für ein festgewähltes Objekt A aus der Kategorie $\mathcal{C}$ können wir in ganz ähnlicher Weise auch einen kontravarianten Funktor $\mathrm{Mor}_{\mathcal{C}}(-,A)\colon \mathcal{C} \longrightarrow \mathcal{M}\!\mathit{c}$ erhalten, in dem wir definieren:

$$\mathrm{Mor}_{\mathcal{C}}(-,A)(B) := \mathrm{Mor}_{\mathcal{C}}(B,A)$$

$$\mathrm{Mor}_{\mathcal{C}}(-,A)(B,C)(f) := \mathrm{Mor}_{\mathcal{C}}(f,A)$$

wobei $\mathrm{Mor}_{\mathcal{C}}(f,A)$ wie in 3.3.4 definiert wird, also als

$$\mathrm{Mor}_{\mathcal{C}}(f,A)\colon \mathrm{Mor}_{\mathcal{C}}(C,A) \ni g \longmapsto gf \in \mathrm{Mor}_{\mathcal{C}}(B,A) \quad .$$

Wir überlassen es dem Leser, sich davon zu überzeugen, daß $\mathrm{Mor}_{\mathcal{C}}(-,A)$ tatsächlich ein kontravarianter Funktor ist. Funktoren der Form $\mathrm{Mor}_{\mathcal{C}}(A,-)$ bzw. $\mathrm{Mor}_{\mathcal{C}}(-,A)$ nennt man auch d a r s t e l l b a r e F u n k t o r e n .

Weitere Beispiele für kovariante Funktoren erhalten wir für jede der Kategorien aus den Beispielen 2 - 14, indem wir den dort genannten mathematischen Objekten die unterliegende Menge und den strukturerhaltenden

Abbildungen ebendiese, aufgefaßt nur als Abbildungen von Mengen, zuordnen. Die so erhaltenen Funktoren werden häufig V e r g i ß f u n k t o r e n genannt. Am Beispiel der Kategorie der Monoide sei das genauer ausgeführt.

Wir definieren $\mathcal{V} : \mathcal{M}o \longrightarrow \mathcal{M}e$ auf folgende Weise. Für ein Monoid $(A,\circ)$ über der Menge A mit der Verknüpfung $\circ$ sei $\mathcal{V}(A,\circ) := A$, also die unterliegende Menge. Für den Monoidhomomorphismus $f: (A,\circ) \longrightarrow (B,*)$ sei $\mathcal{V}((A,\circ),(B,*))(f) := f$, also dieselbe Abbildung $f: A \longrightarrow B$, nur jetzt aufgefaßt als Morphismus in der Kategorie der Mengen. Sicher ist dann $\mathcal{V}((A,\circ),(A,\circ))(id_A) = id_A$ die Identität. Ebenso ist $\mathcal{V}((A,\circ),(C,*))(gf) = gf = \mathcal{V}((B,\times),(C,*))(g)\mathcal{V}((A,\circ),(B,\times))(f)$. Damit ist $\mathcal{V}: \mathcal{M}o \longrightarrow \mathcal{M}e$ ein kovarianter Funktor.

Ähnlich erhält man Vergißfunktoren von der Kategorie der Ringe in die Kategorie der abelschen Gruppen, indem man die Multiplikation der Ringe "vergißt". Wenn wir das Axiom der Kommutativität "vergessen", erhalten wir einen Vergißfunktor $\mathcal{A}\mathcal{K} \longrightarrow \mathcal{G}r$. Wenn wir bei den Ringen mit Einselement die Addition "vergessen", so erhalten wir einen kovarianten Funktor in die Kategorie der Monoide.

Ebenso wie andere strukturerhaltende Abbildungen kann man auch Funktoren hintereinander ausführen. Es gibt auch hier zu jeder Kategorie $\mathcal{C}$ den Identitätsfunktor $Id_{\mathcal{C}}: \mathcal{C} \longrightarrow \mathcal{C}$ mit $Id_{\mathcal{C}}(C) = C$ und $Id_{\mathcal{C}}(A,B)(f) = f$. Wir wollen hier jedoch nicht auf die Details eingehen.

4.2 Funktorielle Morphismen

Den eigentlichen Anstoß zur Definition von Kategorien und Funktoren gab, historisch gesehen, die Notwendigkeit, funktorielle Morphismen, die man

aus wichtigen Beispielen kannte, axiomatisch erfassen zu können. Wir wollen sie hier kurz definieren und an einem Beispiel erläutern.

4.2.1 DEFINITION:
Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien und $\mathcal{F}: \mathcal{C} \longrightarrow \mathcal{D}$ und $\mathcal{G}: \mathcal{C} \longrightarrow \mathcal{D}$ kovariante Funktoren. Ein **funktorieller Morphismus** $\varphi: \mathcal{F} \longrightarrow \mathcal{G}$ ist eine Familie von Morphismen $\varphi(A): \mathcal{F}(A) \longrightarrow \mathcal{G}(A)$ für alle Objekte $A \in \mathrm{Ob}\,\mathcal{C}$, so daß für alle Morphismen $f: A \longrightarrow B$ in $\mathcal{C}$ das Diagramm

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\varphi(A)} & \mathcal{G}(A) \\ \downarrow{\scriptstyle \mathcal{F}(f)} & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(B) & \xrightarrow{\varphi(B)} & \mathcal{G}(B) \end{array}$$

kommutativ ist, d.h. $\varphi(B)\mathcal{F}(f) = \mathcal{G}(f)\varphi(A)$.
Sind $\mathcal{F}$ und $\mathcal{G}$ kontravariante Funktoren, so verlangt man statt $\varphi(B)\mathcal{F}(f) = \mathcal{G}(f)\varphi(A)$ die Beziehung $\varphi(A)\mathcal{F}(f) = \mathcal{G}(f)\varphi(B)$, d.h. die Kommutativität von

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{\varphi(A)} & \mathcal{G}(A) \\ \uparrow{\scriptstyle \mathcal{F}(f)} & & \uparrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(B) & \xrightarrow{\varphi(B)} & \mathcal{G}(B) \end{array} \quad .$$

4.2.2 BEISPIEL für einen funktoriellen Morphismus *):
Als Kategorien wählen wir zweimal die Kategorie $\mathcal{M}e$ der Mengen. Als Funktoren wählen wir $\mathrm{Id}_{\mathcal{M}e}: \mathcal{M}e \longrightarrow \mathcal{M}e$ und $\mathrm{Mor}_{\mathcal{M}e}(\mathrm{Mor}_{\mathcal{M}e}(-,A),A): \mathcal{M}e \longrightarrow \mathcal{M}e$, d.h. die Hintereinanderausführung von $\mathrm{Mor}_{\mathcal{M}e}(-,A)$ mit $\mathrm{Mor}_{\mathcal{M}e}(-,A)$.
Man prüft leicht nach, daß $\mathrm{Mor}_{\mathcal{M}e}(\mathrm{Mor}_{\mathcal{M}e}(-,A),A)$ ein kovarianter Funktor ist. Nun definieren wir

*) Wenn man die hier angegebene Konstruktion analog in der Kategorie der K-Vektorräume durchführt, so erhältman die bekannte K-lineare Abbildung eines Vektorraumes V in seinen Bidual-Raum V**. Diese K-lineare Abbildung kann man tatsächlich auch als funktoriellen Morphismus auffassen.

φ: $Id_{\mathcal{M}e} \longrightarrow Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(-,A),A)$. Für $B \in Ob\,\mathcal{M}e$ ist $\varphi(B)$: $Id_{\mathcal{M}e}(B) \longrightarrow Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(B,A),A)$, also $\varphi(B)$: $B \longrightarrow Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(B,A),A)$ anzugeben. Für $b \in B$ und $f \in Mor_{\mathcal{M}e}(B,A)$ sei

$$\varphi(B)(b)(f) := f(b) \in A \ .$$

Wir müssen jetzt die Kommutativität von

$$\begin{array}{ccc} B & \xrightarrow{\varphi(B)} & Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(B,A),A) \\ \downarrow f & & \downarrow Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(f,A),A) \\ C & \xrightarrow{\varphi(C)} & Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(C,A),A) \end{array}$$

für $f \in Mor_{\mathcal{M}e}(B,C)$ prüfen. Sei dazu $b \in B$ und $g \in Mor_{\mathcal{M}e}(C,A)$. Dann ist

$$Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(f,A),A)\varphi(B)(b)(g) =$$

$$\varphi(B)(b)Mor_{\mathcal{M}e}(f,A)(g) =$$

$$\varphi(B)(b)(gf) =$$

$$gf(b) =$$

$$\varphi(C)f(b)(g) \ .$$

Da das für alle g und b gilt, ist $\varphi(C)f = Mor_{\mathcal{M}e}(Mor_{\mathcal{M}e}(f,A),A)\varphi(B)$.

Natürlich kann man auch wieder funktorielle Morphismen miteinander verknüpfen, und zu jedem Funktor gibt es den identischen funktoriellen Morphismus. Sind $\mathcal{T} : \mathcal{C} \longrightarrow \mathcal{D}$ und $\mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$ Funktoren und sind $\varphi : \mathcal{T} \longrightarrow \mathcal{G}$ und $\psi : \mathcal{G} \longrightarrow \mathcal{T}$ funktorielle Morphismen mit $\varphi\psi = id_{\mathcal{G}}$ und $\psi\varphi = id_{\mathcal{T}}$, so heißen φ bzw. ψ f u n k t o r i e l l e I s o m o r p h i s m e n , und die Funktoren $\mathcal{T}$ und $\mathcal{G}$ heißen funktoriell isomorph. Vieles, was wir im Abschnitt 3 über Morphismen gesagt haben, läßt sich auch für funktorielle Morphismen formulieren und beweisen.

Zum Abschluß wollen wir noch kurz auf das Problem von Isomorphismen zwischen Kategorien eingehen. Es gibt dafür nämlich zwei wichtige verschiedene Begriffe, für die wir zur genauen Definition funk-

torielle Isomorphismen benötigen.

4.2.3 DEFINITION:
Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien und $\mathcal{F}: \mathcal{C} \longrightarrow \mathcal{D}$ und $\mathcal{G}: \mathcal{D} \longrightarrow \mathcal{C}$ Funktoren. $\mathcal{F}$ und $\mathcal{G}$ heißen **Isomorphien**, wenn gilt $\mathcal{G}\mathcal{F} = \mathrm{Id}_{\mathcal{C}}$ und $\mathcal{F}\mathcal{G} = \mathrm{Id}_{\mathcal{D}}$. Existieren zwischen den Kategorien $\mathcal{C}$ und $\mathcal{D}$ Isomorphien, so heißen sie isomorph.

4.2.4 DEFINITION:
Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien und $\mathcal{F}: \mathcal{C} \longrightarrow \mathcal{D}$ und $\mathcal{G}: \mathcal{D} \longrightarrow \mathcal{C}$ Funktoren. $\mathcal{F}$ und $\mathcal{G}$ heißen **Äquivalenzen**, wenn es funktorielle Isomorphismen $\mathcal{G}\mathcal{F} \cong \mathrm{Id}_{\mathcal{C}}$ und $\mathcal{F}\mathcal{G} \cong \mathrm{Id}_{\mathcal{D}}$ gibt. Existieren zwischen den Kategorien $\mathcal{C}$ und $\mathcal{D}$ Äquivalenzen, so heißen sie äquivalent.

Obwohl der Begriff der Isomorphie zunächst der natürlichere zu sein scheint, stellt sich bei Beispielen heraus, daß er sehr eng ist und daß der Begriff der Äquivalenz ein viel wichtigerer und weitertragender ist.

Ein einfaches Beispiel für eine Äquivalenz ist das folgende. Sei $\{\emptyset\} =: E$ eine einpunktige Menge. Den Funktor $\mathrm{Mor}_{\mathcal{M}e}(E,-): \mathcal{M}e \longrightarrow \mathcal{M}e$ haben wir oben schon beschrieben. Nun ist $\varphi: \mathrm{Id}_{\mathcal{M}e} \longrightarrow \mathrm{Mor}_{\mathcal{M}e}(E,-)$ mit $\varphi(A): A \longrightarrow \mathrm{Mor}_{\mathcal{M}e}(E,A)$ definiert durch $\varphi(A)(a)(\emptyset) = a$ für alle $a \in A$ ein funktorieller Isomorphismus mit dem inversen funktoriellen Isomorphismus $\psi: \mathrm{Mor}_{\mathcal{M}e}(E,-) \longrightarrow \mathrm{Id}_{\mathcal{M}e}$, $\psi(A): \mathrm{Mor}_{\mathcal{M}e}(E,A) \longrightarrow A$ und $\psi(A)(f) = f(\emptyset)$. Der Leser möge die Details dieser Behauptung verifizieren. Wir erhalten jedenfalls funktorielle Isomorphismen $\psi: \mathrm{Mor}_{\mathcal{M}e}(E,-)\mathrm{Id}_{\mathcal{M}e} \cong \mathrm{Id}_{\mathcal{M}e}$ und $\psi: \mathrm{Id}_{\mathcal{M}e}\,\mathrm{Mor}_{\mathcal{M}e}(E,-) \cong \mathrm{Id}_{\mathcal{M}e}$. Daher ist $\mathrm{Mor}_{\mathcal{M}e}(E,-)$ eine Äquivalenz mit "inverser" Äquivalenz $\mathrm{Id}_{\mathcal{M}e}$. Man sieht hier, daß die"inverse"Äquivalenz nicht eindeutig bestimmt sein muß. Ein weiteres wichtiges Beispiel liefert die Tatsache, daß die Kategorie

der K-Vektorräume $K\text{-}\mathcal{M}od$ über einem Körper K äquivalent ist zur Kategorie der unitären K-Moduln $R\text{-}\mathcal{M}od$ für den Ring $R = M_2(K)$ der 2×2-Matrizen über K. Ein Beweis davon würde allerdings den hiergegebenen Rahmen sprengen. Die Behauptung impliziert jedoch, daß man mit Objekten und Morphismen in $K\text{-}\mathcal{M}od$ genauso rechnen kann wie in $R\text{-}\mathcal{M}od$. So ist in $R\text{-}\mathcal{M}od$ jeder Monomorphismus ein Schnitt, weil das in $K\text{-}\mathcal{M}od$ der Fall ist. Jedoch hat in $R\text{-}\mathcal{M}od$ nicht jeder Modul eine Basis, wie das in $K\text{-}\mathcal{M}od$ der Fall ist, weil das eine Aussage über die Elemente von Objekten ist, die nicht in den kategorischen Rahmen paßt.

Nicht-triviale Isomorphien erhält man mit Hilfe der Betrachtungen aus IV.4 zwischen den Kategorien der Booleschen Verbände, der Booleschen Ringe und der Booleschen Algebren. Die Funktoren für diese Isomorphien sind auf den Objekten durch IV.4.2.1 und IV.4.2.2 definiert. Der Leser kann sich leicht die Definition für die Morphismen überlegen.

§ 5 Universelle Probleme

5.1 Anfangs- und Endobjekte, Nullobjekte

Universelle Probleme sind, grob gesprochen, Bedingungen für eine Menge von Objekten und Morphismen (evtl. auch in verschiedenen Kategorien, die durch Funktoren verbunden sind), unter denen zwischen zwei Objekten genau ein Morphismus existiert, der die Bedingungen erfüllt. Wir wollen hier keine exakte Definition für universelle Probleme angeben. Ein erstes Beispiel ist dem Leser schon aus der Einleitung dieses Kapitels bekannt. Formal fassen wir es wie folgt:

5.1.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Ein Objekt $A \in \mathrm{Ob}\,\mathcal{C}$ heißt Anfangsobjekt, wenn für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Menge $\mathrm{Mor}_{\mathcal{C}}(A,C)$ aus genau einem Element besteht. Ein Objekt $E \in \mathrm{Ob}\,\mathcal{C}$ heißt Endobjekt, wenn für alle $C \in \mathrm{Ob}\,\mathcal{C}$ die Menge $\mathrm{Mor}_{\mathcal{C}}(C,E)$ aus genau einem Element besteht.

In der Einleitung sahen wir, daß $\emptyset$ in $\mathcal{To}$ und $\mathbb{Z}$ in der Kategorie der Ringe mit Einselement Anfangsobjekte sind. Weiter sind $\emptyset$ in $\mathcal{Me}$, $\{0\}$ in $\mathcal{Mo}$, $\{0\}$ in $\mathcal{Gr}$ und $\{0\}$ in R-$\mathcal{Mod}$ Anfangsobjekte. Endobjekte sind $\{\emptyset\}$ in $\mathcal{Me}$, $\{0\}$ in $\mathcal{Mo}$, $\mathcal{Gr}$, $\mathcal{Ri}$ und R-$\mathcal{Mod}$ und $\{\emptyset\}$ in $\mathcal{To}$. Die entsprechende Struktur auf den angegebenen Mengen ist immer eindeutig bestimmt und leicht anzugeben. In der Kategorie der Ringe mit Einselement ist der Nullring $\{0\}$ (mit $0 = 1$) ein Endobjekt. In der Kategorie der Körper gibt es weder ein Anfangs- noch ein Endobjekt. Der folgende Satz läßt sich wie in der Einleitung dieses Kapitels beweisen.

5.1.2 SATZ:
Sind A und A' Anfangsobjekte in der Kategorie $\mathcal{C}$, so sind A und A' isomorph. Sind E und E' Endobjekte in der Kategorie $\mathcal{C}$, so sind E und E' isomorph.

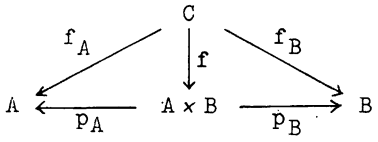
5.1.3 DEFINITION:
Ein Objekt $O \in \mathrm{Ob}\,\mathcal{C}$ heißt N u l l o b j e k t, wenn es Anfangs- und Endobjekt ist.

Nach 5.1.2 ist auch ein Nullobjekt in einer Kategorie bis auf Isomorphie eindeutig bestimmt.

5.2 Produkte und Koprodukte

Obwohl Produkte und Koprodukte für beliebig viele Objekte einer Kategorie $\mathcal{C}$ definiert werden können, so ziehen wir es hier vor, die Definition für jeweils nur zwei Objekte zu geben, da nur die Idee für dieses universelle Problem erläutert werden soll.

5.2.1 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Sei (A,B) ein Paar von Objekten aus $\mathcal{C}$. Ein Objekt, das wir mit $A \times B$ bezeichnen, zusammen mit einem Paar von Morphismen $(p_A: A \times B \longrightarrow A,\ p_B: A \times B \longrightarrow B)$ heißt ein P r o d u k t von A und B, wenn zu jedem Objekt $C \in \mathrm{Ob}\,\mathcal{C}$ und jedem Paar von Morphismen $(f_A: C \longrightarrow A,\ f_B: C \longrightarrow B)$ genau ein Morphismus $f: C \longrightarrow A \times B$ existiert, daß das Diagramm



kommutiert, d.h. daß $p_A f = f_A$ und $p_B f = f_B$.

In der Kategorie der Mengen kann man leicht nachprüfen, daß die Paarmenge $A \times B = \{(a,b) \mid a \in A,\ b \in B\}$

zusammen mit den Abbildungen

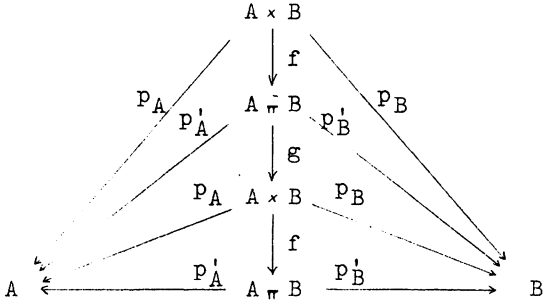
$$p_A: A \times B \ni (a,b) \longmapsto a \in A$$

$$p_B: A \times B \ni (a,b) \longmapsto b \in B$$

ein Produkt im obigen Sinne sind. Auch in vielen anderen Kategorien von mathematischen Objekten kann man die Paarmenge von zwei Objekten mit einer geeigneten Struktur so versehen, daß sie zusammen mit den Abbildungen p_A und p_B ein Produkt ist. Wichtig für die allgemeine Diskussion von Produkten ist nun der folgende Satz.

5.2.2 SATZ:
Seien $(A \times B, p_A, p_B)$ und $(A \pi B, p'_A, p'_B)$ Produkte für das Paar (A,B) von Objekten der Kategorie $\mathcal{C}$. Dann gibt es genau einen Morphismus $f: A \times B \longrightarrow A \pi B$ mit $p'_A f = p_A$ und $p'_B f = p_B$ und dieser ist ein Isomorphismus.

Beweis: Die erste Behauptung für f folgt direkt aus der Eigenschaft, daß $(A \pi B, p'_A, p'_B)$ ein Produkt ist. Es bleibt zu zeigen, daß f ein Isomorphismus ist. Aus Symmetriegründen gibt es genau einen Morphismus $g: A \pi B \longrightarrow A \times B$ mit $p_A g = p'_A$ und $p_B g = p'_B$. Das Diagramm

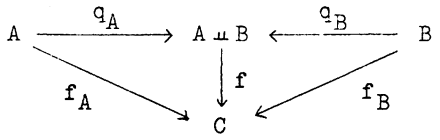


ist also kommutativ. Insbesondere gelten $p_A gf = p_A$, $p_B gf = p_B$ und $p_A \restriction_{A \times B} = p_A$, $p_B \restriction_{A \times B} = p_B$. Da $(A \times B, p_A, p_B)$ ein Produkt ist (in der dritten Zeile des Diagramms), folgt aus der geforderten Eindeutigkeit des Morphismus $A \times B \longrightarrow A \times B$, daß

$gf = 1_{A \times B}$ ist. In bezug auf $(A \pi B, p'_A, p'_B)$ erhält man ebenso, daß $fg = 1_{A \pi B}$ ist. Also ist f ein Isomorphismus. //

Durch Dualisieren (Umkehrung der Morphismenrichtungen) erhalten wir den Begriff des Koprodukts.

5.2.3 DEFINITION:
Sei $\mathcal{C}$ eine Kategorie. Sei (A,B) ein Paar von Objekten aus $\mathcal{C}$. Ein Objekt $A \amalg B$ zusammen mit einem Paar von Morphismen
$(q_A: A \longrightarrow A \amalg B,\ q_B: B \longrightarrow A \amalg B)$ heißt ein K o p r o d u k t von A und B, wenn zu jedem Objekt $C \in \mathrm{Ob}\,\mathcal{C}$ und jedem Paar von Morphismen $(f_A: A \longrightarrow C,\ f_B: B \longrightarrow C)$ genau ein Morphismus $f: A \amalg B \longrightarrow C$ existiert, daß das Diagramm



kommutiert, d.h. daß $fq_A = f_A$ und $fq_B = f_B$.

In der Kategorie der Mengen ist die disjunkte Vereinigung $A \dot\cup B := \{(a,1),(b,2) \mid a \in A, b \in B\}$ zusammen mit den Einbettungsabbildungen

$$q_A: A \ni a \longmapsto (a,1) \in A \dot\cup B$$

$$q_B: B \ni b \longmapsto (b,2) \in A \dot\cup B$$

ein Koprodukt. In anderen Kategorien sind die Koprodukte von mehr oder minder komplizierter Struktur und sollen daher hier nicht näher diskutiert werden. Durch Dualisieren des Beweises von 5.2.2 erhält man

5.2.4 SATZ:
Seien $(A \amalg B, q_A, q_B)$ und $(A * B, q'_A, q'_B)$ Koprodukte für das Paar (A,B) von Objekten der Kategorie $\mathcal{C}$. Dann gibt es genau einen Morphismus $f: A * B \longrightarrow A \amalg B$ mit $fq'_A = q_A$ und $fq'_B = q_B$ und dieser ist ein Isomorphismus.

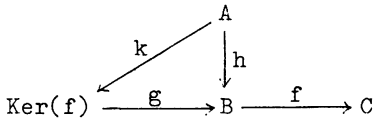
5.3 Kerne und Kokerne

Die Nullabbildungen, d.h. die Abbildungen, die alle Elemente auf das neutrale Element abbilden, in den Kategorien $\mathcal{Mo}$, $\mathcal{Gr}$, $\mathcal{Ab}$ und R-$\mathcal{Mod}$ haben folgende gemeinsamen Eigenschaften. In jeder Morphismenmenge $\mathrm{Mor}_{\mathcal{C}}(A,B)$ gibt es genau einen "Nullmorphismus" $0_{A,B}$. Ist $0_{A,B} \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ ein Nullmorphismus und sind $f \in \mathrm{Mor}_{\mathcal{C}}(B,C)$, $g \in \mathrm{Mor}_{\mathcal{C}}(C,A)$, so sind $f0_{A,B} = 0_{A,C} \in \mathrm{Mor}_{\mathcal{C}}(A,C)$ und $0_{A,B}g = 0_{C,B} \in \mathrm{Mor}_{\mathcal{C}}(C,B)$ Nullmorphismen. Solche Kategorien nennt man auch K a t e g o r i e n m i t N u l l m o r p h i s m e n. Sei $\mathcal{C}$ im folgenden eine Kategorie mit Nullmorphismen.

5.3.1 DEFINITION:
Sei $f: B \longrightarrow C$ ein Morphismus in C. Ein Objekt $\mathrm{Ker}(f)$ zusammen mit einem Morphismus $g: \mathrm{Ker}(f) \longrightarrow B$ heißt ein K e r n von f, wenn gilt:

1) $fg = 0_{\mathrm{Ker}(f),C}$
2) ist $A \in \mathrm{Ob}\,\mathcal{C}$ und $h \in \mathrm{Mor}_{\mathcal{C}}(A,B)$ und gilt $fh = 0_{A,C}$, so existiert genau ein Morphismus $k: A \longrightarrow \mathrm{Ker}(f)$ mit $gk = h$.

Wir erhalten also ein kommutatives Diagramm



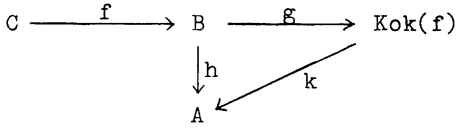
Dual definieren wir

5.3.2 DEFINITION:
Sei $f: C \longrightarrow B$ ein Morphismus in $\mathcal{C}$. Ein Objekt $\mathrm{Kok}(f)$ zusammen mit einem Morphismus $g: B \longrightarrow \mathrm{Kok}(f)$ heißt ein K o k e r n von f, wenn gilt

1) $gf = 0_{C,\mathrm{Kok}(f)}$
2) ist $A \in \mathrm{Ob}\,\mathcal{C}$ und $h \in \mathrm{Mor}_{\mathcal{C}}(B,A)$ und gilt

$hf = 0_{C,A}$, so existiert genau ein Morphismus $k: \mathrm{Kok}(f) \longrightarrow A$ mit $kg = h$.

Wir erhalten also wieder ein kommutatives Diagramm



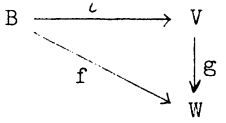
Ebenso wie bei den Produkten und Koprodukten gilt auch hier die Eindeutigkeit von Kernen und Kokernen "bis auf Isomorphie". Wir zitieren den entsprechenden Satz, ohne ihn hier zu beweisen.

5.3.3 SATZ:
Sei $\mathcal{C}$ eine Kategorie mit Nullmorphismen. Sei $f \in \mathrm{Mor}_{\mathcal{C}}(B,C)$. Seien $(\mathrm{Ker}(f),g)$ und $(\mathrm{Ker}(f)',g')$ Kerne von f . Dann gibt es genau einen Morphismus $h: \mathrm{Ker}(f) \longrightarrow \mathrm{Ker}(f)'$ mit $g'h = g$ und dieser ist ein Isomorphismus.
Seien $(\mathrm{Kok}(f),g)$ und $(\mathrm{Kok}(f)',g')$ Kokerne von f . Dann gibt es genau einen Morphismus $h: \mathrm{Kok}(f)' \longrightarrow \mathrm{Kok}(f)$ mit $hg' = g$ und dieser ist ein Isomorphismus.

In den Kategorien $\mathcal{Mo}$, $\mathcal{Gr}$, $\mathcal{AB}$ und R-$\mathcal{Mod}$ ist für $f: B \longrightarrow C$ der Kern jeweils $\{b \mid b \in B \wedge f(b) = 0\}$ zusammen mit der Inklusionsabbildung $\{b \mid b \in B \wedge f(b) = 0\} \rightarrow B$. In $\mathcal{AB}$ und R-$\mathcal{Mod}$ ist der Kokern von $f: B \longrightarrow C$ gegeben durch $C/\mathrm{Bi}(f)$ zusammen mit der Restklassenabbildung $C \longrightarrow C/\mathrm{Bi}(f)$.

Es gibt noch weitere universelle Probleme, auch solche, in denen mehrere Kategorien eine Rolle spielen. Als Beispiel sei nur der folgende Satz über die Basis B eines K-Vektorraumes V genannt.

Zu jedem K-Vektorraum W und jeder Abbildung $f: B \longrightarrow W$ gibt es genau eine K-lineare Abbildung $g: V \longrightarrow W$, so daß das Diagramm



kommutiert.

Um dieses universelle Problem (die Abbildung $B \xrightarrow{\iota} V$ ist universell in bezug auf die Klasse aller Abbildungen $B \longrightarrow W$ für alle K-Vektorräume W) in befriedigender Weise auf allgemeine Kategorien zu übertragen, benötigt man den Begriff des adjungierten Funktors. Der Leser sei für Darstellungen dieser Zusammenhänge auf die Speziallehrbücher verwiesen.

Weitere Beispiele für universelle Probleme findet man in der Konstruktion einer von einem kommutativen Monoid erzeugten kommutativen Gruppe (IV.2.9.2) und in der Konstruktion des Quotientenkörpers (IV.5.2.2).

VII. Kapitel: Aufbau des Zahlensystems

§ 1 Die natürlichen Zahlen

1.1 Die Peanoschen Axiome

In diesem Abschnitt sollen die Eigenschaften der (Menge der) natürlichen Zahlen untersucht werden. Dabei werden wir uns auf die Grundbegriffe der Mengenlehre stützen, wie sie im II. Kapitel eingeführt worden sind. Zwar ist dort von der Menge der natürlichen Zahlen schon gesprochen worden, aber nur in Beispielen, um die neu eingeführten Begriffe zu veranschaulichen. Dort, wo eine der wichtigsten Eigenschaften der natürlichen Zahlen verwendet worden ist, nämlich die (vollständige) Induktion, wurden damit Aussagen bewiesen, die wir in diesem Abschnitt nicht benötigen werden. Durch die frühzeitige Verwendung der Induktion wird hier also kein Zirkelschluß ausgeführt.

Zur Konstruktion der natürlichen Zahlen kann man folgendermaßen vorgehen. Zunächst werden einige Eigenschaften der Menge der natürlichen Zahlen, wie wir sie uns intuitiv vorstellen, ausgewählt und diese dann als Axiome zugrundegelegt. Diese Axiome sollen in der Sprache der Mengenlehre formuliert werden. Da die bisherigen Grundbegriffe der Mengenlehre nicht ausreichen, um nachzuweisen, daß es eine Menge gibt, die den ausgewählten Axiomen genügt, d.h. die ein "Modell" für die Axiome ist, werden wir die Existenz einer solchen Menge als zusätzliches Axiom der Mengenlehre fordern. Die übrigen Eigenschaften der natürlichen Zahlen, insbesondere die Addition, die Multiplikation und die Ordnung, werden dann aus den Axiomen hergeleitet. Bevor wir uns den Axiomen für die natürlichen Zahlen zuwenden, sei hier bemerkt, daß jetzt die Zahl "Null" zur Menge der natürlichen Zahlen hinzugenommen werden soll. Das ist zwar nicht unbe-

dingt erforderlich, bringt aber später bei der Entwicklung der Rechenregeln für die Addition gewisse Vorteile mit sich. Im Unterschied zur Menge $\mathbb{N} = \{1,2,3,\ldots\}$ werden wir die hier zu betrachtende Menge mit $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ bezeichnen. Übrigens kann man dasselbe Axiomensystem, das wir unten zur Einführung von $\mathbb{N}_0$ verwenden werden, auch zur Definition von $\mathbb{N}$ verwenden (denn es gibt offenbar eine ordnungstreue bijektive Abbildung $\mathbb{N}_0 \longrightarrow \mathbb{N}$). Nur müßte man dann die Addition auf etwas andere Weise definieren.

Die wichtigsten Eigenschaften der natürlichen Zahlen, die wir in etwas abgewandelter Form als Axiome verwenden werden, wurden von Peano (1858 - 1932) (und früher auch schon von Dedekind (1831 - 1916) in ähnlicher Fassung) formuliert. Es sind die sogenannten

PEANO AXIOME

(P1) Null ist eine natürliche Zahl.

(P2) Jede natürliche Zahl besitzt einen eindeutig bestimmten Nachfolger, der wieder eine natürliche Zahl ist.

(P3) Null ist nicht Nachfolger einer natürlichen Zahl.

(P4) Natürliche Zahlen mit gleichen Nachfolgern sind gleich.

(P5) (Prinzip der vollständigen Induktion:) Eine Eigenschaft, die der Null zukommt und mit einer beliebigen natürlichen Zahl auch ihrem Nachfolger, kommt allen natürlichen Zahlen zu.

Man wird sofort bemerken, daß in diesen Peano Axiomen außer den logischen und mengentheoretischen Begriffen auch einige undefinierte Begriffe vorkommen, wie "Null", "natürliche Zahl", "Nachfolger". Wir wollen diese Axiome daher in der Sprache der Mengenlehre noch weiter formalisieren. Die Axiome (P1) und (P3) sagen im wesentlichen, daß die Null ein besonders ausgezeichnetes Element von $\mathbb{N}_0$ ist. (P2) sagt, daß die Bildung des Nachfolgers eine Abbildung von $\mathbb{N}_0$ in $\mathbb{N}_0$ ist. (P4) sagt, daß die Nachfolger-Abbildung eine injektive Abbildung ist.

1.1.1 DEFINITION:
Ein Tripel (A,a_o,μ), bestehend aus einer Menge A, einem Element $a_o \in A$ und einer Abbildung $\mu: A \longrightarrow A$, das den folgenden Axiomen genügt:

(P'3) $\forall\, x \in A \left[\mu(x) \neq a_o\right]$

(P'4) μ ist eine injektive Abbildung

(P'5) $\forall\, E \in P(A)^{*)} \left[a_o \in E \wedge (\forall\, x \in E \left[\mu(x) \in E\right]) \Longrightarrow E = A\right]$

heißt "Menge der natürlichen Zahlen".

In dieser Definition sind die Axiome jetzt nur mit schon definierten Begriffen ausgedrückt. Die Existenz einer Menge der natürlichen Zahlen müssen wir jedoch über die bisherigen Axiome der Mengenlehre hinaus noch fordern:

(M 6) Es existiert eine Menge der natürlichen Zahlen.

Eine nach (M 6) existierende Menge der natürlichen Zahlen werden wir fortan mit $(\mathbb{N}_o, 0, \nu)$ bezeichnen.

Das Axiom (P'5) sagt aus, daß unter allen möglichen Modellen (A,a_o,μ), die die Axiome (P'3) und (P'4) erfüllen, die Menge der natürlichen Zahlen ein minimales Modell ist. (P'5) beinhaltet aber auch eine der wichtigsten Beweistechniken, den Beweis durch vollständige Induktion.

1.1.2 SATZ über den Beweis durch vollständige Induktion
Für jedes $n \in \mathbb{N}_o$ sei eine mathematische Aussage $A(n)$ formuliert. Dafür gelte
(Induktionsanfang:) $A(0)$ ist richtig und
(Induktionsannahme:) aus der Richtigkeit von $A(n)$
(Induktionsschluß:) folgt die Richtigkeit von $A(\nu(n))$.
Dann ist $A(n)$ für alle $n \in \mathbb{N}_o$ richtig.

Beweis: Sei $E = \{x \mid x \in \mathbb{N}_o \wedge A(x)$ richtig$\}$. Es gilt $0 \in E$ und $\forall\, x \in E \left[\nu(x) \in E\right]$. Nach (P'5) folgt $E = \mathbb{N}_o$. //

*) $P(A)$ = Potenzmenge von A

Für spätere Zwecke überlegen wir noch, daß jedes Element $\neq 0$ aus $\mathbb{N}_0$ Nachfolger ist.

1.1.3 LEMMA:
$\forall\, n \in \mathbb{N}_0 \left[n \neq 0 \iff \exists\, m \in \mathbb{N}_0 \left[\nu(m) = n \right] \right]$.

Beweis: "$\Longrightarrow$": Sei $A(n)$ die Aussage

$$n = 0 \vee \exists\, m \in \mathbb{N}_0 \left[\nu(m) = n \right] .$$

Dann gilt $A(0)$ und für jedes n gilt $A(\nu(n))$. Nach 1.1.2 gilt folglich $A(n)$ für jedes $n \in \mathbb{N}_0$.
"$\Longleftarrow$": Nach (P'3) ist $\nu(m) \neq 0$ für jedes $m \in \mathbb{N}_0$, also gilt $\nu(m) = n \neq 0$. //

1.2 Die Eindeutigkeit der Menge der natürlichen Zahlen

Sei $(\mathbb{N}_0, 0, \nu)$ eine Menge der natürlichen Zahlen. Dann ist auch $(\mathbb{N}_0^*, 0^*, \nu^*)$ eine Menge der natürlichen Zahlen, wenn

$$\mathbb{N}_0^* := \{x^* \mid x \in \mathbb{N}_0\}$$

und

$$\nu^*(x^*) := \nu(x)^*$$

gesetzt werden. Da $(\mathbb{N}_0, 0, \nu)$ und $(\mathbb{N}_0^*, 0^*, \nu^*)$ verschieden sind, gibt es also nicht nur eine Menge der natürlichen Zahlen. Allerdings ist dieser Unterschied durch "Umbenennung" entstanden und daher nicht von Bedeutung für die Struktur der Menge der natürlichen Zahlen. Wir wollen nun zeigen, daß dies für zwei beliebige Mengen der natürlichen Zahlen gilt. Mit anderen Worten: Zwei beliebige Mengen der natürlichen Zahlen sind "isomorph" bezüglich ihrer Struktur. Um das zu zeigen, benötigen wir zunächst den Begriff des Abschnitts und zwei Hilfssätze.

Eine Teilmenge $A \subset \mathbb{N}_0$ heißt ein Abschnitt von $\mathbb{N}_0$, wenn $0 \in A$ und $\forall\, y \in \mathbb{N}_0 \left[\nu(y) \in A \Longrightarrow y \in A \right]$.

1.2.1 LEMMA:
Seien A ein Abschnitt von $\mathbb{N}_0$, X eine Menge und

$f,g : A \longrightarrow X$ Abbildungen, für die gilt

1) $f(0) = g(0)$

2) $\forall\, a \in A \left[\nu(a) \in A \wedge f(a) = g(a) \Longrightarrow f(\nu(a)) = g(\nu(a))\right]$.

Dann ist $f = g$.

Beweis: Sei $A' = \mathbb{N}_0 \setminus A$ und $E = A' \cup \{a \in A \mid f(a) = g(a)\}$. Wir wollen $E = \mathbb{N}_0$ zeigen. Dann ist nämlich $A = \{a \in A \mid f(a) = g(a)\}$, also $f = g$. Es ist $0 \in E$ wegen der Voraussetzung $f(0) = g(0)$. Sei $x \in E$. Wir wollen zeigen, daß $\nu(x) \in E$. Ist $\nu(x) \in A'$, so gilt $\nu(x) \in E$. Ist $\nu(x) \notin A'$, so ist $\nu(x) \in A$, also auch $x \in A$, da A ein Abschnitt ist. Wegen $x \in E$ gilt also $f(x) = g(x)$. Nach Voraussetzung 2) folgt $f(\nu(x)) = g(\nu(x))$. Also ist $\nu(x) \in E$. Nach (P'5) ist $E = \mathbb{N}_0$ .//

1.2.2 LEMMA:
Seien X eine Menge, $x_0 \in X$ und $\varphi: X \longrightarrow X$ eine Abbildung. Dann gibt es genau eine Abbildung $f: \mathbb{N}_0 \longrightarrow X$ mit

(1) $f(0) = x_0$

(2) $\forall\, a \in \mathbb{N}_0 \left[f(\nu(a)) = \varphi(f(a))\right]$.

Bemerkung: Die Eigenschaft (2) besagt, daß das Diagramm

$$\begin{array}{ccc} \mathbb{N}_0 & \xrightarrow{\nu} & \mathbb{N}_0 \\ \downarrow f & & \downarrow f \\ X & \xrightarrow{\varphi} & X \end{array}$$

kommutativ ist. Um die Bedeutung von (2) klar zu machen, greifen wir den folgenden Überlegungen vor und setzen $a + 1 := \nu(a)$. Dann kann (2) so verstanden werden, daß f induktiv durch

$$f(a + 1) := \varphi(f(a))$$

bzw. durch $f(a) = \varphi^a(x_0)$ definiert wird. Man sagt auch, daß f durch einfache Rekursion aus φ hervorgeht. Selbstverständlich ist mit dieser erklärenden Bemerkung kein Beweis geliefert.

Beweis von 1.2.2: Sei $\mathfrak{M}$ die Menge aller Abschnitte A von $\mathbb{N}_0$, für die eine Abbildung $f: A \longrightarrow X$ mit

$$(*)\quad \begin{cases} f(0) = x_0 \\ \forall\, a \in A \left[\nu(a) \in A \Longrightarrow f(\nu(a)) = \varphi(f(a))\right] \end{cases}$$

existiert. Mit Hilfe von Lemma 1.2.1 stellen wir fest, daß diese Abbildung f durch (*) eindeutig bestimmt ist. Sei auch $g: A \longrightarrow X$ mit (*), dann gilt $f(0) = x_0 = g(0)$ und falls $\nu(a) \in A$ und bereits $f(a) = g(a)$ gilt, dann folgt

$$f(\nu(a)) = \varphi(f(a)) = \varphi(g(a)) = g(\nu(a)).$$

Nach 1.2.1 ist dann $f = g$.

Für

$$E := \bigcup_{A \in \mathfrak{M}} A$$

soll nun $E = \mathbb{N}_0$ gezeigt werden. Definiert man $f: \{0\} \ni 0 \longmapsto x_0 \in X$, so folgt $\{0\} \in \mathfrak{M}$, also $0 \in E$. Sei $a \in E$, dann existiert ein $A \in \mathfrak{M}$ mit $a \in A$. Ist $\nu(a) \in A$, dann ist $\nu(a) \in E$. Ist $\nu(a) \notin A$, dann betrachten wir $A_1 := A \cup \{\nu(a)\}$. Offensichtlich ist A_1 wieder ein Abschnitt, da A ein Abschnitt ist und $a \in A \subset A_1$. Ist f die zu A gehörende Abbildung mit (*), dann sei

$$f_1: A_1 \longrightarrow X$$

definiert durch

$$f_1 | A := f \wedge f_1(\nu(a)) := \varphi(f(a)).$$

Dann erfüllt f_1 die Bedingung (*), d.h. $A_1 \in \mathfrak{M}$ und $\nu(a) \in E$. Nach (P'5) folgt $E = \mathbb{N}_0$.

Wir definieren nun $f: \mathbb{N}_0 \longrightarrow X$ wie folgt. Sei $a \in \mathbb{N}_0 (= E)$. Dann gibt es ein $A_1 \in \mathfrak{M}$ mit $a \in A_1$. $f_1: A_1 \longrightarrow X$ sei die zugehörige Abbildung, die (*) erfüllt. Wir setzen $f(a) := f_1(a)$ und zeigen, daß $f(a)$ nicht von der Wahl von $A_1 \in \mathfrak{M}$ mit $a \in A_1$ abhängt. Sei auch $A_2 \in \mathfrak{M}$ mit $a \in A_2$ und sei $f_2: A_2 \longrightarrow X$ die zugehörige Abbildung, die (*) erfüllt. Dann ist auch $A_1 \cap A_2$ ein Abschnitt und $f_1 | A_1 \cap A_2$ so wie $f_2 | A_1 \cap A_2$ erfüllen beide die

Bedingungen dafür, daß $A_1 \cap A_2 \in \mathfrak{M}$ gilt. Wegen der Eindeutigkeit (1.2.1) folgt $f_1 | A_1 \cap A_2 = f_2 | A_1 \cap A_2$, also $f_1(a) = f_2(a)$, denn $a \in A_1 \cap A_2$.

Die damit definierte Abbildung $f: \mathbb{N}_0 \longrightarrow X$ erfüllt $f(0) = x_0$. Für $a \in \mathbb{N}_0$ sei A_1 ein Abschnitt mit $\nu(a) \in A_1 \in \mathfrak{M}$. Wie zuvor im Beweis gezeigt, gibt es einen solchen Abschnitt. Für die zugehörige Abbildung f_1 gilt dann $f_1(\nu(a)) = \varphi(f_1(a))$, also gilt diese Bedingung auch für f. Insbesondere folgt $\mathbb{N}_0 \in \mathfrak{M}$ und daher ist, wie anfangs festgestellt, f eindeutig bestimmt. //

Damit können wir die Eindeutigkeit der Menge der natürlichen Zahlen "bis auf Isomorphie" beweisen.

1.2.3 SATZ
Seien $(\mathbb{N}_0, 0, \nu)$ und (A, a_0, μ) jeweils eine Menge der natürlichen Zahlen (im Sinne von Definition 1.1.1). Dann gibt es genau eine bijektive Abbildung $f: \mathbb{N}_0 \longrightarrow A$, für die gilt

(1) $f(0) = a_0$

(2) $\forall\, n \in \mathbb{N}_0 \; \left[f(\nu(n)) = \mu(f(n))\right]$.

Beweis: Wendet man Lemma 1.2.2 auf $X = A$, $x_0 = a_0$ und $\varphi = \mu$ an, so erhält man genau eine Abbildung f, die die Bedingungen (1) und (2) erfüllt. Symmetrisch erhält man $g: A \longrightarrow \mathbb{N}_0$ mit $g(a_0) = 0$ und

$$\forall\, a \in A \; \left[g(\mu(a)) = \nu(g(a))\right] .$$

Die Abbildung $gf: \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ erfüllt nun $gf(0) = 0$ und

$$\forall\, n \in \mathbb{N}_0 \; \left[gf(\nu(n)) = \nu(gf(n))\right] .$$

Dieselben Bedingungen erfüllt auch $id_{\mathbb{N}_0}: \mathbb{N}_0 \longrightarrow \mathbb{N}_0$. Wegen der Eindeutigkeit in Lemma 1.2.2 (mit $X = \mathbb{N}_0$, $x_0 = 0$ und $\varphi = \nu$) erhält man $gf = id_{\mathbb{N}_0}$. Symmetrisch erhält man $fg = id_A$. Also ist f bijektiv. //

1.3 Die Addition der natürlichen Zahlen

Lemma 1.2.2 können wir auch zur Definition der Addition und der Multiplikation der natürlichen Zahlen verwenden. Wir beginnen hier mit der Addition.

1.3.1 DEFINITION:
Für $m \in \mathbb{N}_0$ sei $f_m : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ die durch Lemma 1.2.2 für $X = \mathbb{N}_0$, $x_0 = m$ und $\varphi = \nu$ eindeutig bestimmte Abbildung mit

$$f_m(0) = m$$

$$f_m(\nu(n)) = \nu(f_m(n)) \quad \text{für alle} \quad n \in \mathbb{N}_0 .$$

Dann wird für alle $m,n \in \mathbb{N}_0$ definiert:

$$m + n := f_m(n) .$$

1.3.2 FOLGERUNG:
Für alle $m,n \in \mathbb{N}_0$ gilt:

$$m + \hat{0} = m ,$$

$$m + \nu(n) = \nu(m + n) .$$

Daß mit dieser Definition tatsächlich die Addition im gewünschten Sinne definiert wird, zeigt der folgende Satz. Darin und im folgenden setzen wir wie üblich $1 := \nu(0)$.

1.3.3 SATZ:
Für alle $m,n,r \in \mathbb{N}_0$ gelten:

(1) $m + 0 = m = 0 + m$,
(2) $m + 1 = \nu(m)$,
(3) $m + \nu(n) = \nu(m + n) = \nu(m) + n$,
(4) $m + n = n + m$,
(5) $(m + n) + r = m + (n + r)$,
(6) $m + n = m + r \Longrightarrow n = r$,
(7) $m + n = 0 \Longrightarrow m = n = 0$.

Beweis: Beim Beweis benutzen wir die schon bewiesenen Gleichungen ohne Hinweis.

(1) $m + 0 = m$ gilt nach 1.3.2. Durch Induktion nach

m beweisen wir $0+m=m$. Die Aussage $A(m)$ im Sinne von 1.1.2 sei dazu $0+m=m$.
Induktionsanfang: $0+0=0$ gilt bereits als Spezialfall von $m+0=m$.
Induktionsannahme: Es gelte $0+m=m$.
Induktionsschluß: Nach 1.3.2 folgt aus $0+m=m$

$$0+\nu(m)=\nu(0+m)=\nu(m).$$

(2) Wir hatten $1:=\nu(0)$ definiert. Dann folgt mit Hilfe von 1.3.2

$$m+1=m+\nu(0)=\nu(m+0)=\nu(m).$$

(3) Nach 1.3.2 gilt $m+\nu(n)=\nu(m+n)$. Wir zeigen die zweite Gleichung durch Induktion nach n für alle m.
Induktionsanfang: $m+\nu(0)=m+1=\nu(m)=\nu(m)+0$.
Induktionsannahme: Es gelte $m+\nu(n)=\nu(m)+n$ für alle $m\in\mathbb{N}_0$.
Induktionsschluß: $m+\nu(\nu(n))=\nu(m+\nu(n))=\nu(\nu(m)+n)=\nu(m)+\nu(n)$.

(4) Wir zeigen durch Induktion nach n für alle m: $m+n=n+m$.
Induktionsanfang: $m+0=m=0+m$.
Induktionsannahme: Es gelte schon $m+n=n+m$ für alle $m\in\mathbb{N}_0$.
Induktionsschluß: $m+\nu(n)=\nu(m+n)=\nu(n+m)=\nu(n)+m$.

(5) Wir zeigen durch Induktion nach m für alle $n,r\in\mathbb{N}_0$: $(m+n)+r=m+(n+r)$.
Induktionsanfang: $(0+n)+r=n+r=0+(n+r)$.
Induktionsannahme: Es gelte $(m+n)+r=m+(n+r)$ für alle $n,r\in\mathbb{N}_0$.
Induktionsschluß: $(\nu(m)+n)+r=\nu(m+n)+r=\nu((m+n)+r)=\nu(m+(n+r))=\nu(m)+(n+r)$.

(6) Wir zeigen die Behauptung durch Induktion nach m für alle $n,r\in\mathbb{N}_0$.

Induktionsanfang: Aus $0+n=0+r$ folgt nach (1) $n=r$.
Induktionsannahme: Die Behauptung gelte für m und für alle $n,r\in\mathbb{N}_0$.
Induktionsschluß: $\nu(m)+n=\nu(m)+r \Longrightarrow \nu(m+n)=\nu(m+r)$. Wegen (P'4) folgt daraus $m+n=m+r$ und die Annahme ergibt $n=r$.

(7) Angenommen $m\neq 0$, dann existiert nach 1.1.3 ein $a\in\mathbb{N}_0$ mit $m=\nu(a) \Longrightarrow 0=m+n=\nu(a)+n=\nu(a+n)$ im Widerspruch zu (P'3). //

Dieser Satz zeigt, daß $(\mathbb{N}_0,+)$ ein kommutatives Monoid mit 0 als neutralem Element ist. Wir sagen, daß ein kommutatives Monoid $(M,*)$ die Kürzungseigenschaft hat, wenn

$$\forall\, m,n,r\in M\ [m*n=m*r \Longrightarrow n=r]$$

gilt. Nach (6) des Satzes ist $(\mathbb{N}_0,+)$ ein kommutatives Monoid mit Kürzungseigenschaft.

1.4 Definition der Ordnung der natürlichen Zahlen

1.4.1 DEFINITION:
Wir definieren eine Relation $\leq$ auf $\mathbb{N}_0$ durch

$$\forall\, m,n\in\mathbb{N}_0\ [m\leq n :\Longleftrightarrow \exists\, r\in\mathbb{N}_0\ [r+m=n]]\ .$$

1.4.2 BEHAUPTUNG
Die Relation $\leq$ auf $\mathbb{N}_0$ ist eine Wohlordnung.

Beweis: 1. Reflexivität: $\forall\, n\in\mathbb{N}_0\ [0+n=n] \Longrightarrow \forall\, n\in\mathbb{N}_0\ [n\leq n]$.
2. Transitivität: Gelte $m\leq n$ und $n\leq s$ für $m,n,s\in\mathbb{N}_0$. $\Longrightarrow \exists\, r,t\in\mathbb{N}_0\ [r+m=n\wedge t+n=s] \Longrightarrow (t+r)+m=t+(r+m)=t+n=s \Longrightarrow \exists\, u\in\mathbb{N}_0\ [u+m=s] \Longrightarrow m\leq s$.
3. Antisymmetrie: Für $m,n\in\mathbb{N}_0$ gelte $m\leq n$ und $n\leq m$. $\Longrightarrow \exists\, r,s\in\mathbb{N}_0\ [r+m=n\wedge s+n=m] \Longrightarrow (r+s)+n=r+(s+n)=r+m=0+n \Longrightarrow r+s=0$ (wegen 1.3.3 (6)). Nach 1.3.3 (7) folgt $r=s=0$, also $m=r+m=n$.

4. $\leq$ ist eine Wohlordnung: Sei $M \subset \mathbb{N}_0$ ohne kleinstes Element. Es ist $M = \emptyset$ zu zeigen. Sei $E := \{x \mid x \in \mathbb{N}_0 \wedge \forall\, m \in M\ [x \leq m]\}$. Da M kein kleinstes Element besitzt, ist $E \cap M = \emptyset$, denn $y \in E \cap M \Longrightarrow \forall\, m \in M\ [y \leq m]$, was der Annahme über M widerspricht. Es ist sicher $0 \in E$. Sei $x \in E$ und $m \in M$. $\Longrightarrow \exists\, r \in \mathbb{N}_0\ [r + x = m]$. Sicher ist $r \neq 0$, denn sonst wäre $x = m \in E \cap M = \emptyset$. Damit ist $r = \nu(s)$ und $s + \nu(x) = \nu(s) + x = r + x = m$, also $\nu(x) \leq m$. Mit $x \in E$ ist also auch $\nu(x) \in E$ und damit $E = \mathbb{N}_0$. Wegen $E \cap M = \emptyset$ folgt $M = \emptyset$. //

1.4.3 SATZ (I. Monotoniegesetz):

$$\forall\, m,n,r \in \mathbb{N}_0\ [m \leq n \Longrightarrow r + m \leq r + n]\ .$$

Beweis: $m \leq n \Longrightarrow t + m = n \Longrightarrow t + r + m = r + t + m = r + n \Longrightarrow r + m \leq r + n$. //

Aus dem I. Monotoniegesetz folgt sofort die Aussage

$$\forall\, m,n,s,t \in \mathbb{N}_0\ [m \leq n \wedge s \leq t \Longrightarrow m + s \leq n + t]\ ,$$

denn $m + s \leq m + t = t + m \leq t + n = n + t$.

1.4.4 FOLGERUNG:

$$\forall\, n \in \mathbb{N}_0\ [n \neq 0 \Longrightarrow 1 \leq n]\ .$$

Beweis: Nach 1.1.3 existiert ein $m \in \mathbb{N}_0$ mit $n = \nu(m)$. Aus $0 \leq m$ folgt $0 + 1 = 1 \leq m + 1 = \nu(m) = n$. //

1.5 Die Multiplikation der natürlichen Zahlen

1.5.1 DEFINITION:
Für $m \in \mathbb{N}_0$ sei $g_m : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ die durch Lemma 1.2.2 für $X = \mathbb{N}_0$, $x_0 = 0$ und

$$\varphi_m : \mathbb{N}_0 \ni r \longmapsto r + m \in \mathbb{N}_0$$

eindeutig bestimmte Abbildung mit

$$g_m(0) = 0$$

$$g_m(\nu(n)) = \varphi_m(g_m(n)) \quad \text{für alle } n \in \mathbb{N}_0$$

Dann wird für alle $m,n \in \mathbb{N}_0$ definiert:

$$mn := g_m(n) .$$

1.5.2 FOLGERUNG:
Für alle $m,n \in \mathbb{N}_0$ gilt:

$$m0 = 0 ,$$

$$m\nu(n) = m(n+1) = mn + m .$$

Daß mit dieser Multiplikation tatsächlich die Multiplikation im gewünschten Sinne definiert wird, zeigt der folgende Satz.

1.5.3 SATZ:
Für alle $m,n,r \in \mathbb{N}_0$ gilt:

(1) $m0 = 0 = 0m$,
(2) $(m+1)n = mn + n$,
(3) $mn = nm$,
(4) $m(n+r) = mn + mr$,
(5) $m(nr) = (mn)r$,
(6) $1n = n = n1$,
(7) $m \neq 0 \wedge n \neq 0 \Rightarrow mn \neq 0$,
(8) $m \neq 0 \wedge mn = mr \Rightarrow n = r$.

Beweis: (1) $m0 = 0$ gilt nach 1.5.2. Wir beweisen $0m = 0$ durch Induktion nach m .
Induktionsanfang: $00 = 0$ nach 1.5.2.
Induktionsannahme: Es gelte $0m = 0$.
Induktionsschluß: Wegen 1.5.2 gilt $0\nu(m) = 0m + 0 = 0 + 0 = 0$.

(2) Induktion nach n für alle $m \in \mathbb{N}_0$.
Induktionsanfang: $(m+1)0 = 0 = m0 + 0$.
Induktionsannahme: Es gelte $(m+1)n = mn + n$.
Induktionsschluß: Bei Beachtung von 1.5.2 folgt $(m+1)(n+1) = (m+1)n + (m+1) = (mn + n) + (m+1) = (mn + m) + (n+1) = m(n+1) + (n+1)$.

(3) Induktion nach n für alle $m \in \mathbb{N}_0$.
Induktionsanfang: $m0 = 0 = 0m$.
Induktionsannahme: $mn = nm$.

Induktionsschluß: $m(n+1) = mn + m = nm + m = (n+1)m$.

(4) Induktion nach r für alle m und n .

(5) Induktion nach r für alle m und n . Die Ausführung der Induktionsbeweise von (4) und (5) bleibt dem Leser zur Übung überlassen.

(6) $1n = n$ folgt aus (2) für $m = 0$ und mit (3) folgt $n = n1$.

(7) Aus $m \neq 0$ und $n \neq 0$ folgt nach 1.1.3, daß $a,b \in \mathbb{N}_0$ mit $m = \nu(a) = a + 1$ und $n = \nu(b) = b + 1$ existieren. Dann folgt $mn = (a+1)(b+1) = (ab + a + b) + 1 = \nu(ab + a + b)$, also $mn \neq 0$ nach 1.1.3.

(8) Ohne Einschränkung kann $n \leq r$ angenommen werden. Folglich existiert ein $t \in \mathbb{N}_0$ mit $n + t = r$. Damit erhält man $mn + 0 = mn = mr = m(n+t) = mn + mt$ und 1.3.3 (6) ergibt $0 = mt$. Wegen $m \neq 0$ und (7) folgt $t = 0$, also $n = r$. //

Der folgende Satz gibt einen Zusammenhang zwischen der Ordnung von $\mathbb{N}_0$ und der Multiplikation.

1.5.4 SATZ (II. Monotoniegesetz):

$$\forall\ m,n,r \in \mathbb{N}_0\ \left[r \neq 0 \Longrightarrow (m \leq n \Longleftrightarrow rm \leq rn)\right] .$$

Beweis: "$\Longrightarrow$": Sei $m \leq n$, dann existiert ein $t \in \mathbb{N}_0$ mit $m + t = n$. Es folgt $rm + rt = rn$, also $rm \leq rn$. "$\Longleftarrow$": Sei $rm \leq rn$. Angenommen $n \leq m$, dann folgt, wie schon bewiesen, $rn \leq rm$, also gilt $rm = rn$ und nach 1.5.3 (8) folgt $m = n$. //

§ 2 Die ganzen Zahlen

2.1 Definition, Addition und Multiplikation der ganzen Zahlen

Zur Einführung der Menge $\mathbb{Z}$ der ganzen Zahlen verfahren wir anders als bei den natürlichen Zahlen. Statt $\mathbb{Z}$ axiomatisch zu beschreiben, wird $\mathbb{Z}$ mit Hilfe von $\mathbb{N}_0$ konstruiert.

Das Problem, das zur Erweiterung von $\mathbb{N}_0$ zu $\mathbb{Z}$ führt, besteht darin, daß die Umkehrung der Addition in $\mathbb{N}_0$ nicht unbeschränkt durchführbar ist. Es sind also die Inversen bezüglich der Addition zu $\mathbb{N}_0$ hinzuzufügen. Die dazu notwendige Konstruktion haben wir bereits allgemein in IV.2.9.2 kennen gelernt. Sie liefert, angewendet auf $\mathbb{N}_0$, die von $\mathbb{N}_0$ erzeugte kommutative Gruppe.

2.1.1 DEFINITION:
Sei $(\mathbb{Z},+)$ die von $(\mathbb{N}_0,+)$ im Sinne von IV.2.9.2 erzeugte kommutative Gruppe. $\mathbb{Z}$ heißt Menge der g a n z e n Z a h l e n . Die Elemente von $\mathbb{Z}$ werden zunächst in der Form $\overline{(m,n)}$ mit $m,n \in \mathbb{N}_0$ geschrieben.

2.1.2 DEFINITION und LEMMA:
Für $\overline{(m,n)},\overline{(s,t)} \in \mathbb{Z}$ wird die Multiplikation durch

$$\overline{(m,n)}\,\overline{(s,t)} := \overline{(ms+nt,ns+mt)}$$

definiert und diese Definition ist unabhängig von der Auswahl der Repräsentanten.

Beweis: Sei $\overline{(m,n)} = \overline{(m',n')}$ und $\overline{(s,t)} = \overline{(s',t')} \Longrightarrow$
$m+n' = m'+n$ und $t+s' = t'+s \Longrightarrow m(s+t')+n(t+s')$
$+ (m+n')s' + (n+m')t' = m(t+s')+n(s+t')+(n+m')s'$
$+ (m+n')t' \Longrightarrow ms+nt+n's'+m't'+mt'+ns'+ms'+nt'$
$= m's'+n't'+ns+mt+mt'+ns'+ms'+nt' \Longrightarrow$
$ms+nt+n's'+m't' = m's'+n't'+ns+mt \Longrightarrow$
$\overline{(ms+nt,ns+mt)} = \overline{(m's'+n't',n's'+m't')}$. //

Zum Verständnis dieser Definition beachte man, daß

später (2.2) $\overline{(m,n)} = m - n$ gelten wird und daß dann $\overline{(m,n)}\,\overline{(s,t)} = (m-n)(s-t) = ms + nt - ns - mt = \overline{(ms+nt,ns+mt)}$ folgt.

2.1.3 SATZ:
$\mathbb{Z}$ ist mit der in 2.1.2 definierten Multiplikation ein kommutativer Ring mit Eins-Element.

Beweis: a) $((\overline{(m,n)}\,\overline{(s,t)})\,\overline{(u,v)} = \overline{(ms+nt,ns+mt)}\,\overline{(u,v)} = \overline{(msn+ntu+nsv+mtv,nsu+mtu+msv+ntv)} = \overline{(m,n)}\,\overline{(su+tv,tu+sv)} = \overline{(m,n)}(\overline{(s,t)}\,\overline{(u,v)})$.

b) $\overline{(1,0)}\,\overline{(m,n)} = \overline{(m,n)} = \overline{(m,n)}\,\overline{(1,0)}$.

c) $\overline{(m,n)}\,\overline{(s,t)} = \overline{(ms+nt,ns+mt)} = \overline{(sm+tn,tm+sn)} = \overline{(s,t)}\,\overline{(m,n)}$.

d) $\overline{(m,n)}(\overline{(s,t)} + \overline{(u,v)}) = \overline{(m,n)}\,\overline{(s+u,t+v)} = \overline{(ms+mu+nt+nv,ns+nu+mt+mv)} = \overline{(m,n)}\,\overline{(s,t)} + \overline{(m,n)}\,\overline{(u,v)}$. Das zweite Distributivgesetz gilt jetzt wegen c). //

2.2 Einbettung von $\mathbb{N}_0$ und Ordnung auf $\mathbb{Z}$

Nach IV.2.9.1 ist der Gruppenhomomorphismus $f: \mathbb{N}_0 \longrightarrow \mathbb{Z}$ injektiv, denn es gilt

$$\forall\, m,n,r \in \mathbb{N}_0 \left[m + n = m + r \Longrightarrow n = r \right]$$

(siehe 1.3.3 (6)).

Für $n \in \mathbb{N}_0$ gilt $f(n) = \overline{(n,0)}$. Wegen $\overline{(n,0)} + \overline{(0,n)} = \overline{(n,n)} = \overline{(0,0)}$ folgt $-\overline{(n,0)} = \overline{(0,n)}$. Wir beweisen nun, daß man alle Elemente aus $\mathbb{Z}$ in der Form $\overline{(n,0)}$ oder $-\overline{(n,0)} = \overline{(0,n)}$ mit $n \in \mathbb{N}_0$ erhält. Sei $\overline{(m,n)} \in \mathbb{Z}$ und sei zuerst $n \leq m$. Dann existiert ein $t \in \mathbb{N}_0$ mit $m = n + t$. Es folgt $\overline{(m,n)} = \overline{(n+t,n)} = \overline{(t,0)}$. Ist hingegen $m < n$, so existiert $t \in \mathbb{N}_0$ mit $m + t = n$. Es folgt $\overline{(m,n)} = \overline{(m,m+t)} = \overline{(0,t)}$.

Da $f: \mathbb{N}_0 \longrightarrow \mathbb{Z}$ injektiv ist, gilt für $m \neq n$ auch $\overline{(m,0)} \neq \overline{(n,0)}$, und, da $\mathbb{Z}$ eine Gruppe ist, folgt für die inversen Elemente ebenfalls $\overline{(0,m)} \neq \overline{(0,n)}$.

Für $m \neq 0$ und $n \in \mathbb{N}_0$ gilt schließlich $\overline{(m,0)} \neq \overline{(0,n)}$. Ist nämlich $\overline{(m,0)} = \overline{(0,n)}$, so folgt nach Definition der Äquivalenzrelation $m + n = 0$. Nach 1.3.3 (7) folgt $m = n = 0$.

Da f injektiv ist, wollen wir $n \in \mathbb{N}_0$ mit $f(n) = \overline{(n,0)}$ identifizieren, so daß $\mathbb{N}_0$ bezüglich der Addition ein Untermonoid von $\mathbb{Z}$ wird. Nach obiger Überlegung ist auch $f^-: \mathbb{N}_0 \ni n \longmapsto \overline{(0,n)} \in \mathbb{Z}$ injektiv. Wir schreiben $f^-(n) = \overline{(0,n)} = -\overline{(n,0)} = -n$ mit der Identifizierung zwischen n und $\overline{(n,0)}$.

Die vorhergehenden Überlegungen können wir dann folgendermaßen zusammenfassen.

2.2.1 BEMERKUNG:

$$\mathbb{Z} = \mathbb{N}_0 \cup \{-n \mid n \in \mathbb{N}_0 \wedge n \neq 0\}$$

als disjunkte Vereinigung.

Wie üblich bezeichnen wir die Zahlen der Menge

$$\mathbb{Z}^- := \{-n \mid n \in \mathbb{N}_0 \wedge n \neq 0\}$$

als **negative ganze Zahlen**.

2.2.2 BEMERKUNG:
Die in 2.1.2 definierte Multiplikation auf $\mathbb{Z}$ setzt die Multiplikation von $\mathbb{N}_0$ fort. Es gilt für alle $m,n \in \mathbb{N}_0$:

$$mn = \overline{(mn,0)} = \overline{(m,0)}\overline{(n,0)} .$$

Weiter gelten für alle $m,n \in \mathbb{N}_0$

$$(-m)n = \overline{(0,m)}\overline{(n,0)} = \overline{(0,mn)} = -(mn) ,$$

$$m(-n) = \overline{(m,0)}\overline{(0,n)} = \overline{(0,mn)} = -(mn) ,$$

$$(-m)(-n) = \overline{(0,m)}\overline{(0,n)} = \overline{(mn,0)} = mn .$$

Seien $N \subset Z$ Mengen und sei auf N eine Ordnung definiert. Eine Ordnung auf Z heißt eine **Fortsetzung** der Ordnung auf N, wenn ihre Einschränkung auf N die vorgegebene Ordnung auf N ist. Wir wollen jetzt die Ordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$ fortsetzen.

2.2.3 SATZ:
Die folgende Relation auf $\mathbb{Z}$

$$\forall\ x,y\in\mathbb{Z}\ \left[x\leq y :\Longleftrightarrow y-x\in\mathbb{N}_0\right]$$

ist eine totale Ordnung und eine Fortsetzung der Ordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$.

Beweis: 1. Reflexivität: $x\leq x$ wegen $x-x=0\in\mathbb{N}_0$ für alle $x\in\mathbb{Z}$.
2. Transitivität: $x\leq y$ und $y\leq z \Longrightarrow y-x\,,\,z-y\in\mathbb{N}_0$ $\Longrightarrow (z-y)+(y-x)=z-x\in\mathbb{N}_0 \Longrightarrow x\leq z$.
3. Antisymmetrie: $x\leq y$ und $y\leq x \Longrightarrow y-x, x-y\in\mathbb{N}_0 \wedge$ $0=(y-x)+(x-y)\in\mathbb{N}_0 \Longrightarrow y-x=0 \Longrightarrow x=y$.
4. Totale Ordnung: $\forall\ x,y\in\mathbb{Z}\ \left[x-y\in\mathbb{N}_0 \vee y-x\in\mathbb{N}_0\right] \Longrightarrow$ $\forall\ x,y\in\mathbb{Z}\ \left[y\leq x \vee x\leq y\right]$.
5. Fortsetzung der Ordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$:
$\forall\ m,n\in\mathbb{N}_0\ \left[m\leq n \text{ in } \mathbb{N}_0 \Longleftrightarrow \exists\ t\in\mathbb{N}_0\ \left[t+m=n\right]\right] \Longleftrightarrow$ $n-m\in\mathbb{N}_0 \Longleftrightarrow m\leq n \text{ in } \mathbb{Z}\left]\right.$. //

2.2.4 SATZ:
Im Ring $\mathbb{Z}$ gelten folgende Rechenregeln:
a) I. Monotoniegesetz:

$$\forall\ x,y,z\in\mathbb{Z}\ \left[x\leq y \Longrightarrow z+x\leq z+y\right] ,$$

b) II. Monotoniegesetzt:

$$\forall\ x,y\in\mathbb{Z},\ r\in\mathbb{N}_0\ \left[x\leq y \Longrightarrow rx\leq ry\right] ,$$

c) Nullteilerfreiheit:

$$\forall\ x,y\in\mathbb{Z}\ \left[x\neq 0\wedge y\neq 0 \Longrightarrow xy\neq 0\right] .$$

Beweis: a) $x\leq y \Longrightarrow y-x\in\mathbb{N}_0 \Longrightarrow (z+y)-(z+x)\in\mathbb{N}_0$ $\Longrightarrow z+x\leq z+y$.

b) $x\leq y \Longrightarrow y-x\in\mathbb{N}_0 \Longrightarrow r(y-x)=ry-rx\in\mathbb{N}_0 \Longrightarrow$ $rx\leq ry$.

c) Gilt nach 1.5.3 (7) für $x,y\in\mathbb{N}_0\setminus\{0\}$. Dann folgt für $m,n\in\mathbb{N}_0\setminus\{0\}$ auch $(-m)n=m(-n)=-(mn)\neq 0$, $(-m)(-n)=mn\neq 0$. //

2.2.5 FOLGERUNG:

a) $\forall\ x,y,z\in\mathbb{Z}\ \left[z\neq 0\wedge zx=zy \Longrightarrow x=y\right]$,

b) $\forall\, x \in \mathbb{Z}\ \left[0 \leq xx =: x^2\right]$,

c) $\forall\, x,y \in \mathbb{Z}\,,\ r \in \mathbb{N}_0\ \left[r \neq 0 \Longrightarrow \left[x \leq y \Longleftrightarrow rx \leq ry\right]\right]$.

Beweis: a) $zx = zy \Longrightarrow zx - zy = z(x-y) = 0$; da $z \neq 0$ $\Longrightarrow x - y = 0 \Longrightarrow x = y$.
b) Ist $0 \leq x \Longrightarrow 0 = 0x \leq xx$ nach dem II. Monotoniegesetz. Ist $x \leq 0$, dann folgt $0 \leq 0 - x = -x$, also $0 \leq (-x)(-x) = xx$.
c) "$\Longrightarrow$" gilt nach dem II. Monotoniegesetz.
"$\Longleftarrow$": $rx \leq ry \Longrightarrow ry - rx = r(y-x) \in \mathbb{N}_0$. Angenommen $y \leq x \Longrightarrow ry \leq rx \Longrightarrow rx = ry$ wegen der Antisymmetrie. $\Longrightarrow x = y$ wegen a), also folgt $x \leq y$ aus $rx \leq ry$. //

2.2.6 SATZ: (Division mit Rest)

$$\forall\, x \in \mathbb{Z},\ n \in \mathbb{N}_0 \setminus \{0\}\ \dot{\exists}\ q_0 \in \mathbb{Z},\ r \in \mathbb{N}_0\ \left[r \leq n-1 \wedge x = q_0 n + r\right]$$

und in dieser Darstellung sind q_0 und r durch x und n eindeutig bestimmt.

Beweis: Existenz von q_0 und r . Sei

$$M := \{x - qn \mid q \in \mathbb{Z} \wedge 0 \leq x - qn\}\ .$$

Dann gilt $M \subset \mathbb{N}_0$ und $M \neq \emptyset$. Ist nämlich $0 \leq x$, so folgt $x \in M$ (mit $q = 0$); ist jedoch $x \leq 0$, so folgt $x - xn = x(1-n) = (-x)(n-1) \geq 0$, also $x - xn \in M$ (mit $q = x$). Da $\mathbb{N}_0$ wohlgeordnet ist, existiert ein kleinstes Element $r \in M$. Das zugehörige q sei q_0 , d.h. es gelte $x - q_0 n = r$. Angenommen $n \leq r$, dann existiert ein $t \in \mathbb{N}_0$ mit $n + t = r$. Wegen $1 \leq n$ muß $t \leq r - 1$ gelten. Dann folgt $x = q_0 n + r = q_0 n + n + t = (q_0 + 1)n + t$, also $x - (q_0 + 1)n = t$ im Widerspruch zur Minimalität von r . Es muß also $r \leq n - 1$ gelten.

Eindeutigkeit von q_0 und r . Gelte $a = q_0 n + r = q'n + r'$ mit $q_0, q' \in \mathbb{Z}$, $r, r' \in \mathbb{N}_0$, $r \leq n-1$, $r' \leq n-1$. Ohne Einschränkung kann $r \leq r'$ angenommen werden. Dann folgt

$$0 \leq r' - r = (q_0 - q')n \leq n - 1\ ,$$

also gilt $0n \leq (q_o - q')n$ und wegen 2.2.5 c) folgt $0 \leq q_o - q'$. Nimmt man $1 \leq q_o - q'$ an, so folgt $n \leq (q_o - q')n$ im Widerspruch zu $(q_o - q')n \leq n - 1$. Also folgt wegen 1.4.4 $q_o - q' = 0$, d.h. $q_o = q'$ und folglich auch $r = r'$. //

§ 3 Der Körper der rationalen Zahlen

3.1 Definition des Körpers der rationalen Zahlen

Um von den natürlichen Zahlen zu den ganzen Zahlen zu gelangen, mußten, wie wir in § 2 gesehen haben, zur Menge $\mathbb{N}_0$ die fehlenden negativen Zahlen hinzugefügt werden. Ähnlich gelangt man von den ganzen Zahlen zu den rationalen Zahlen. Jetzt müssen zur Menge $\mathbb{Z}$ die fehlenden inversen Zahlen hinzugefügt werden. Diese Konstruktion des Quotientenkörpers haben wir bereits allgemein in IV.5.2 kennen gelernt.

3.1.1 DEFINITION:
Sei $(\mathbb{Q},+,\cdot)$ der Quotientenkörper von $(\mathbb{Z},+,\cdot)$ im Sinne von IV.5.2 . $\mathbb{Q}$ heißt der Körper der **rationalen Zahlen** .

3.2 Die Ordnung von $\mathbb{Q}$

Es soll die Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$ fortgesetzt werden. Ehe wir eine genaue Definition der Ordnung auf $\mathbb{Q}$ angeben, überlegen wir uns, daß für die übliche Ordnung auf $\mathbb{Q}$ gilt:

$$\frac{r}{s} \leq \frac{x}{y} \wedge z \in \mathbb{N}_0 \Longrightarrow z \cdot \frac{r}{s} = z \cdot \frac{x}{y} \ .$$

Durch geeignetes $z \in \mathbb{N}_0$ sollte man die Nenner zum Verschwinden bringen können, so daß wir schließlich auf die schon definierte Ordnung von $\mathbb{Z}$ zurückkommen. Da das Produkt der Nenner sy auch in $\mathbb{Z}^-$ liegen könnte, wählen wir $z = s^2y^2$. Dann ist gleichzeitig $z \neq 0$, so daß wir in Analogie zu 2.9 Folgerung c) erwarten können, daß die folgende Definition den gewünschten Sachverhalt richtig wiedergibt.

3.2.1 DEFINITION und LEMMA:
Die folgende Relation auf $\mathbb{Q}$

$$\forall \ \frac{r}{s},\frac{x}{y} \in \mathbb{Q} \ \left[\frac{r}{s} \leq \frac{x}{y} :\Longleftrightarrow rsy^2 \leq xys^2 \ \text{ in } \mathbb{Z}\right]$$

ist eine totale Ordnung und eine Fortsetzung der Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$.

Beweis: 1. Unabhängigkeit der Definition von der

Wahl der Repräsentanten (r,s) bzw. (x,y) für $\frac{r}{s}$ bzw. $\frac{x}{y}$: Sei $(r,s)\sim(r',s')$ und $(x,y)\sim(x',y')$ $\Longrightarrow rs' = r's$ und $xy' = x'y \Longrightarrow [rsy^2 \leq xys^2 \Longleftrightarrow rsy^2(s'y')^2 \leq xys^2(s'y')^2 \Longleftrightarrow r's'y'^2(sy)^2 \leq x'y's'^2(sy)^2 \Longleftrightarrow r's'y'^2 \leq x'y's'^2]$.

2. Reflexivität: $\frac{r}{s} \leq \frac{r}{s}$ wegen $rs^3 \leq rs^3$ in $\mathbb{Z}$ für alle $\frac{r}{s} \in \mathbb{Q}$.

3. Transitivität: $\frac{r}{s} \leq \frac{u}{v}$ und $\frac{u}{v} \leq \frac{x}{y} \Longrightarrow rsv^2 \leq uvs^2$ und $uvy^2 \leq xyv^2 \Longrightarrow rsv^2y^2 \leq uvs^2y^2 \leq xyv^2s^2 \Longrightarrow rsy^2 \leq xys^2$ wegen $v^2 \neq 0$, $v^2 \geq 0$ und 2.2.5 c) $\Longrightarrow \frac{r}{s} \leq \frac{x}{y}$.

4. Antisymmetrie: $\frac{r}{s} \leq \frac{x}{y}$ und $\frac{x}{y} \leq \frac{r}{s} \Longrightarrow rsy^2 \leq xys^2$ und $xys^2 \leq rsy^2 \Longrightarrow rsy^2 = xys^2 \Longrightarrow \frac{r}{s} = \frac{x}{y}$, da man in $\mathbb{Q}$ durch $s^2y^2 \neq 0$ dividieren kann.

5. Totale Ordnung: $\forall\ \frac{r}{s},\frac{x}{y} \in \mathbb{Q}\ [rsy^2 \leq xys^2 \vee xys^2 \leq rsy^2$ in $\mathbb{Z}] \Longrightarrow \forall\ \frac{r}{s},\frac{x}{y} \in \mathbb{Q}\ [\frac{r}{s} \leq \frac{x}{y} \vee \frac{x}{y} \leq \frac{r}{s}]$.

6. Fortsetzung der Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$: $\forall\ r,x \in \mathbb{Z}\ [r \leq x$ in $\mathbb{Z} \Longleftrightarrow r\cdot 1^3 \leq x\cdot 1^3$ in $\mathbb{Z} \Longleftrightarrow \frac{r}{1} \leq \frac{x}{1}$ in $\mathbb{Q}]$. //

3.2.2 SATZ:
Im Körper $\mathbb{Q}$ gelten folgende Rechenregeln:
a) (I. Monotoniegesetz) $\forall\ a,b,c \in \mathbb{Q}\ [a \leq b \Longrightarrow a + c \leq b + c]$,
b) (II. Monotoniegesetz) $\forall\ a,b,c \in \mathbb{Q}\ [a \leq b \wedge 0 \leq c \Longrightarrow ac \leq bc]$.

Beweis: a) Seien $a = \frac{r}{s}$, $b = \frac{u}{v}$, $c = \frac{x}{y}$. Dann gilt $\frac{r}{s} \leq \frac{u}{v} \Longrightarrow rsv^2 \leq uvs^2 \Longrightarrow rsv^2y^4 + xs^2v^2y^3 \leq uvs^2y^4 + xs^2v^2y^3 \Longrightarrow (ry + xs)sv^2y^3 \leq (uy + xv)vs^2y^3 \Longrightarrow \frac{ry + xs}{sy} \leq \frac{uy + xv}{vy} \Longrightarrow \frac{r}{s} + \frac{x}{y} \leq \frac{u}{v} + \frac{x}{y} \Longrightarrow a + c \leq b + c$.

b) Mit der Bezeichnungsweise von a) gilt $a \leq b \Longrightarrow \frac{r}{s} \leq \frac{u}{v} \Longrightarrow rsv^2 \leq uvs^2$. Wegen $c = \frac{x}{y} \geq 0$ gilt $xy^3 \geq 0$. $\Longrightarrow rsv^2xy^3 \leq uvs^2xy^3 \Longrightarrow \frac{rx}{sy} \leq \frac{ux}{vy} \Longrightarrow ac \leq bc$. //

3.2.3 DEFINITION:
Ein Körper K, auf dem eine totale Ordnung $\leq$ so definiert ist, daß die beiden Monotoniegesetze

$$\text{I. } \forall\, a,b,c \in K\ [a \leq b \Longrightarrow a + c \leq b + c]$$

$$\text{II. } \forall\, a,b,c \in K\ [a \leq b \quad 0 \leq c \Longrightarrow ac \leq bc]$$

gelten, heißt ein angeordneter Körper.

Wegen 3.2.2 ist $\mathbb{Q}$ ein angeordneter Körper. Wie wir später sehen werden, bilden auch die reellen Zahlen einen angeordneten Körper. Daher wollen wir weitere Eigenschaften von $\mathbb{Q}$ gleich allgemein für angeordnete Körper K behandeln. Dabei sei $a < b$ definiert durch $a \leq b$ und $a \neq b$. In einem angeordneten Körper K gelten die folgenden

3.2.4 RECHENREGELN:
a) $\forall\, a \in K\ [0 \leq a \Longleftrightarrow -a \leq 0]$,
b) $\forall\, a \in K\ [0 \leq a^2]$,
c) für $2 := 1 + 1$ gilt $0 < 1 < 2$, (man beachte hier, daß wir nicht $\mathbb{Z} \subset K$ annehmen)
d) $\forall\, a \in K\ [0 < a \Longrightarrow 0 < a^{-1}]$,
e) $\forall\, a,b,c \in K\ [0 < c \Longrightarrow [a \leq b \Longleftrightarrow ac \leq bc]]$,
f) $\forall\, a,b \in K\ [a < b \Longrightarrow a < \frac{a+b}{2} < b]$.

Beweis: a) $0 \leq a \Longrightarrow -a + 0 \leq -a + a \Longrightarrow -a \leq 0 \Longrightarrow a - a \leq 0 \Longrightarrow 0 \leq a$.
b) Ist $0 \leq a \Longrightarrow 0 \cdot a \leq a \cdot a \Longrightarrow 0 \leq a^2$. Ist $a \leq 0 \Longrightarrow 0 \leq -a \Longrightarrow 0 \leq (-a)^2 = a^2$.
c) K Körper $\Longrightarrow 0 \neq 1 \Longrightarrow 0 \leq 1^2 = 1 \Longrightarrow 0 < 1 \Longrightarrow 1 \leq 2$. Wäre $1 = 2$, so wäre $0 = 1$, Widerspruch $\Longrightarrow 1 < 2$.
d) Sicher ist $0 \neq a^{-1}$. Wäre $a^{-1} \leq 0 \quad a^{-1} \cdot a = 1 \leq 0 \cdot a = 0$, Widerspruch zu $0 < 1$. Also ist $0 < a^{-1}$.
e) $0 < c \Longrightarrow 0 < c^{-1} \Longrightarrow [a \leq b \Longrightarrow ac \leq bc]$ nach dem II. Monotoniegesetz und ebenso $ac \leq bc \Longrightarrow acc^{-1} \leq bcc^{-1} \Longrightarrow a \leq b$.
f) Zunächst folgt aus c) $0 \neq 2$, denn $0 = 2$ ergäbe $0 \leq 1 \wedge 1 \leq 0$, also $0 = 1$. Damit ist

$$\frac{a+b}{2} = \frac{a}{2} + \frac{b}{2} := (a + b) \cdot 2^{-1}$$

definiert. Nun gilt

$$0 < \frac{1}{2} \Longrightarrow \left[a < b \Longleftrightarrow \frac{a}{2} < \frac{b}{2} \Longleftrightarrow \frac{a}{2} + \frac{a}{2} < \frac{a}{2} + \frac{b}{2} < \frac{b}{2} + \frac{b}{2}\right.$$

$$\left. \Longleftrightarrow \quad a < \frac{a+b}{2} < b \right] .$$

Gleichheit an irgendeiner Stelle würde wegen der Umkehrbarkeit der vorgenommenen Operationen an allen Stellen Gleichheit induzieren. //

3.3 Der absolute Betrag

Für angeordnete Körper führen wir jetzt die folgenden Abbildungen ein:

den Betrag $K \ni x \longmapsto |x| \in K$ mit $|x| = \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x \leq 0 \end{cases}$

das Signum (= Vorzeichen) $\operatorname{sgn}: K \longrightarrow K$ mit

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{für } x > 0 \\ 0 & \text{für } x = 0 \\ -1 & \text{für } x < 0 . \end{cases}$$

3.3.1 RECHENREGELN:

a) $\forall\ x \in K \left[\operatorname{sgn}(x) \cdot |x| = x \wedge |x| = x \cdot \operatorname{sgn}(x)\right]$,

b) $\forall\ x \in K \left[0 = |x| \wedge \left[0 = |x| \Longleftrightarrow 0 = x\right]\right]$,

c) $\forall\ x,y \in K \left[|x + y| \leq |x| + |y|\right]$,

d) $\forall\ x,y \in K \left[|xy| = |x||y|\right]$.

Beweis: a) ist klar nach Definition.

b) folgt ebenfalls direkt aus der Definition.

c) Es gelten nach Definition $x \leq |x|$, $-x \leq |x|$, $y \leq |y|$, $-y \leq |y|$. $\Longrightarrow x + y \leq |x| + |y|$ und $-(x + y) \leq |x| + |y| \Longrightarrow |x + y| \leq |x| + |y|$.

d) Wegen des II. Monotoniegesetzes sieht man leicht: $\operatorname{sgn}(xy) = \operatorname{sgn}(x)\operatorname{sgn}(y)$ für alle $x,y \in K$. Damit erhält man für alle $x,y \in K$

$$|xy| = \operatorname{sgn}(xy) \cdot xy = \operatorname{sgn}(x) \cdot x \cdot \operatorname{sgn}(y) \cdot y = |x| \cdot |y| \quad . //$$

3.3.2 BEMERKUNG:

Für den Körper $\mathbb{Q}$ der rationalen Zahlen erwähnen wir noch eine weitere wichtige Eigenschaft, die nicht in allen angeordneten Körpern gilt:

$$\forall s,t \in \mathbb{Q}\ [0 < s \Longrightarrow \exists n \in \mathbb{N}_0\ [t < ns]]\ .$$

Ein angeordneter Körper mit dieser Eigenschaft wird auch **archimedisch** genannt.

Beweis: Gilt $t \leq s$, dann folgt wegen $0 < s$:
$t \leq s < 2s$.
Sei jetzt $0 < s < t$ und seien $s = \frac{x}{y}$, $t = \frac{u}{v}$ mit $x,y,u,v \in \mathbb{Z}$. Dann gilt $0 < \frac{x}{y} < \frac{u}{v} \Longrightarrow 0 < xyv^2 < uvy^2 \Longrightarrow$
$1 \leq xyv^2 \Longrightarrow uvy^2 < uvy^2 + 1 \leq (uvy^2 + 1)xyv^2 \Longrightarrow$
$\frac{u}{v} < (uvy^2 + 1)\frac{x}{y}$, also $t < ns$ mit $n = uvy^2 + 1$. //

§ 4 Der Aufbau der reellen Zahlen mit Cauchy-Folgen

Die Menge der reellen Zahlen müssen wir mit anderen Hilfsmitteln einführen, als die Menge der ganzen oder rationalen Zahlen. Bisher haben wir nur Erweiterungen des Zahlbereichs benötigt, um gewisse algebraische Operationen wie Addition und Multiplikation umkehren zu können. Bekanntlich läßt sich die Umkehrung einer weiteren algebraischen Operation, des Potenzierens, in der Form des sogenannten Wurzelziehens von positiven rationalen Zahlen in den reellen Zahlen durchführen, doch ist weder die Quadratwurzel von -1 in den reellen Zahlen enthalten, noch läßt sich die transzendente Zahl π in Form einer Wurzel darstellen.

Der Aufbau der reellen Zahlen stützt sich auf eine Grenzwertbildung und ist damit von topologischer, statt von algebraischer Natur. Das Prinzip wird bei der Betrachtung der Zahl $\pi = 3{,}14159265358979323846\ldots$ klar. Dem Leser dürfte bekannt sein, daß die letzten drei Punkte andeuten, daß es nicht möglich ist, π als Dezimalbruch mit nur endlich vielen Stellen hinter dem Komma zu schreiben, noch daß sich die verwendeten Ziffern bei der Dezimaldarstellung von irgendeiner Stelle an periodisch wiederholen. Für fast alle technischen Zwecke ist wiederum die obige zwanzigstellige Angabe von π zu genau. Man kann je nach dem Verwendungszweck auskommen mit

$3{,}1$; $3{,}14$; $3{,}141$; $3{,}1415$; $3{,}14159$; $3{,}141592$ ...

und weiß dann, daß die n-te Zahl in dieser Folge von rationalen (!) Zahlen um höchstens 10^{-n} von π abweicht.

Die Schreibweise der reellen Zahlen in Form von "unendlichen" Dezimalbrüchen ist also nichts anderes

als eine angenäherte Angabe der reellen Zahl mit Hilfe von gewissen rationalen Zahlen, nämlich endlichen Dezimalbrüchen, bis auf eine geforderte Genauigkeit. Man könnte nun zunächst daran denken, die reellen Zahlen als Folgen von Dezimalbrüchen einzuführen, wobei man (wie oben bei der Darstellung von π) jedes folgende Folgenglied aus dem vorhergehenden durch Anfügen einer weiteren Dezimalziffer erhält Das bringt gewisse Schwierigkeiten mit sich. Bekanntlich sind die reellen Zahlen 3,0000... und 2,9999.. (mit sich jeweils wiederholenden Ziffern) gleich obwohl sie durch verschiedene Folgen rationaler Zahlen angenähert werden. Weiter weiß man zunächst nicht, ob die Dezimalschreibweise andere reelle Zahlen ergibt, als etwa die Dualschreibweise (nur mit den Ziffern 0 und 1). Schließlich läßt sich die Addition von so dargestellten reellen Zahlen, deren Zffern alle größer als 5 sind, schwer beschreiben, die Beschreibung der Multiplikation ist noch problematischer. Wir betrachten daher eine wesentlich größere Klasse von Folgen rationaler Zahlen und führen darauf eine Äquivalenzrelation ein, die dann beim Übergang zu den Äquivalenzklassen auch klärt, warum 3,0000... = 2,9999... gilt. Die Konstruktion wollen wir wieder allgemeiner für einen angeordneten Körper K vornehmen.

Die hier angegebene Konstruktion des Körpers der reellen Zahlen ist nicht die einzig mögliche. Einen etwas leichteren Zugang bietet die Konstruktion mit Hilfe von Dedekind'schen Schnitten. Jedoch ist die von uns angegebene Konstruktion der Menge der reellen Zahlen als Vervollständigung bezüglich Cauchy-Folgen rationaler Zahlen ein auch in vielen anderen Gebieten der Mathematik wichtiges Verfahren.

4.1 Cauchy-Folgen

Es sei im folgenden K ein beliebiger angeordneter Körper (3.2.3).

4.1.1 DEFINITION:

a) Eine Folge $(x_n \mid x_n \in K \wedge n \in \mathbb{N}_o)$ heißt Cauchy-Folge oder Fundamentalfolge $:\Longleftrightarrow$

$$\forall\, \varepsilon \in K\ ,\ \varepsilon > 0\ \exists\, n_o \in \mathbb{N}_o\ \forall\, m,n \in \mathbb{N}_o$$
$$\left[n_o \leq m \wedge n_o \leq n \Longrightarrow |x_m - x_n| < \varepsilon\right] .$$

b) Eine Folge $(x_n \mid x_n \in K \wedge n \in \mathbb{N}_o)$ heißt konvergent mit dem Grenzwert $x \in K$ $:\Longleftrightarrow$

$$\forall\, \varepsilon \in K\ ,\ \varepsilon > 0\ \exists\, n_o \in \mathbb{N}_o\ \forall\, n \in \mathbb{N}_o$$
$$\left[n_o \leq n \Longrightarrow |x_n - x| < \varepsilon\right] .$$

c) Eine Folge $(x_n \mid x_n \in K \wedge n \in \mathbb{N}_o)$ heißt Nullfolge $:\Longleftrightarrow$ die Folge ist konvergent mit dem Grenzwert $0 \in K$.

Für die Folge $(x_n \mid x_n \in K \wedge n \in \mathbb{N}_o)$ schreiben wir auch kurz (x_n). Ist die Folge (x_n) konvergent mit dem Grenzwert x, so wird $x = \lim(x_n)$ oder auch

$$x = \lim_{n \in \mathbb{N}_o}(x_n) = \lim_{n \to \infty}(x_n) = \lim_{n \to \infty} x_n$$

geschrieben.

4.1.2 FOLGERUNG:

a) Der Grenzwert einer konvergenten Folge ist eindeutig bestimmt.

b) Genau dann ist die Folge (x_n) konvergent mit dem Grenzwert x, wenn $(x_n - x)$ eine Nullfolge ist.

c) Jede konvergente Folge ist eine Cauchy-Folge.

d) Jede Cauchy-Folge ist beschränkt.

Beweis: a) Indirekter Beweis: Angenommen, es gibt Grenzwerte x,y mit $x \neq y$ von (x_n). Setzt man $\varepsilon := \frac{1}{2}|x - y|$, dann ist $\varepsilon > 0$ und nach Voraussetzung existiert $n \in \mathbb{N}_o$, so daß sowohl $|x_n - x| < \varepsilon$ als

auch $|x_n - y| < \varepsilon$ gelten. Daraus folgt

$$|x - y| = |x - x_n + x_n - y|$$
$$\leq |x - x_n| + |x_n - y| < 2\varepsilon = |x - y| ,$$

also ein Widerspruch.

b) klar nach Definition.

c) Sei $x = \lim(x_n)$. Zu $\varepsilon > 0$ sei $n_o \in \mathbb{N}_o$ so gewählt, daß $|x_n - x| < \frac{\varepsilon}{2}$ für alle $n \geq n_o$ gilt. Für $m \geq n_o$ und $n \geq n_o$ folgt dann

$$|x_m - x_n| = |x_m - x + x - x_n|$$
$$= |x_m - x| + |x - x_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon .$$

d) Nach Voraussetzung gibt es zu $\varepsilon = 1$ ein $n_o \in \mathbb{N}_o$, so daß $|x_m - x_n| < 1$ für alle $m,n \geq n_o$ gilt; speziell gilt also $|x_n - x_{n_o}| < 1$. Daraus folgt $|x_n| < 1 + |x_{n_o}|$ für alle $n \geq n_o$. Damit ergibt sich für alle $n \in \mathbb{N}_o$

$$|x_n| < 1 + \max\{|x_i| \mid i = 0,1,\ldots,n_o\} . \quad //$$

Zur Vorbereitung von späteren Überlegungen beweisen wir jetzt noch einige weitere Eigenschaften von Cauchy-Folgen.

4.1.3 HILFSSATZ:
Sei (x_n) eine Cauchy-Folge, die keine Nullfolge ist. Dann existiert ein $\delta > 0$, $\delta \in K$ und ein $k_o \in \mathbb{N}_o$, so daß genau eine der beiden folgenden Aussagen erfüllt ist:

$$\forall\, n \geq k_o \,[x_n > \delta] , \quad \forall\, n \geq k_o \,[-x_n > \delta] .$$

Beweis: Da (x_n) keine Nullfolge ist, gibt es ein $\varepsilon > 0$, $\varepsilon \in K$, so daß zu jedem $n_o \in \mathbb{N}_o$ ein $n_o' \geq n_o$ mit $|x_{n_o'} - 0| = |x_{n_o'}| \geq \varepsilon$ existiert. Da (x_n) Cauchy-Folge ist, gibt es zu diesem ε ein $k_o \in \mathbb{N}_o$, so daß $|x_m - x_n| < \frac{\varepsilon}{2}$ für alle $m,n \geq k_o$ gilt. Sei $k_o' \geq k_o$ mit $|x_{k_o'}| \geq \varepsilon$, dann folgt wegen

$$|x_{k_o'}| = |x_{k_o'} - x_n + x_n| \leq |x_{k_o'} - x_n| + |x_n|$$

für alle $n \geq k_o$

$$|x_n| \geq |x_{k_o'}| - |x_{k_o'} - x_n| > \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2} .$$

Gilt $x_{m_o} \geq 0$ für ein $m_o \geq k_o$, so folgt $x_{m_o} = |x_{m_o}| > \frac{\varepsilon}{2}$. Für alle $n \geq k_o$ folgt dann $x_n = x_{m_o} - (x_{m_o} - x_n) \geq x_{m_o} - |x_{m_o} - x_n| > \frac{\varepsilon}{2} - \frac{\varepsilon}{2} = 0$, also $x_n = |x_n| > \frac{\varepsilon}{2}$. Folglich sind für $n \geq k_o$ entweder alle x_n positiv oder alle x_n negativ. Im negativen Fall folgt aus $|x_n| > \frac{\varepsilon}{2}$ die Ungleichung $-x_n > \frac{\varepsilon}{2}$. Also ist für $\delta := \frac{\varepsilon}{2}$ und k_o die Behauptung erfüllt. //

Die weiteren Eigenschaften betreffen Teilfolgen von Cauchy-Folgen. Intuitiv betrachtet erhält man aus einer Folge eine Teilfolge, indem man aus der Folge sukzessiv unendlich viele Glieder herausgreift und diese neu durchnumeriert. Es folgt die mathematische Formulierung für diesen Sachverhalt.

4.1.4 DEFINITION:
Die Folge (y_n) heißt Teilfolge der Folge (x_n) $:\Longleftrightarrow$ es existiert eine eigentlich monoton wachsende Abbildung $\tau : \mathbb{N}_o \longrightarrow \mathbb{N}_o$, so daß $y_n = x_{\tau(n)}$ für alle $n \in \mathbb{N}_o$ gilt.

Für die eigentlich monoton wachsende Abbildung τ folgt durch Induktion nach n, daß $n \leq \tau(n)$ für alle $n \in \mathbb{N}_o$ gilt. Davon wird mehrfach Gebrauch gemacht.

Im folgenden bezeichnen wir mit $C(K)$ bzw. $N(K)$ die Menge aller Cauchy-Folgen bzw. Nullfolgen mit Elementen in K.

4.1.5 HILFSSATZ:
Sind $(x_n) \in C(K)$ und (y_n) eine Teilfolge von (x_n), dann gilt:
a) $(y_n) \in C(K)$,
b) $(x_n - y_n) \in N(K)$.

Beweis: a) Zu $\varepsilon > 0$ existiert ein n_o mit

$$\forall\, m,n \geq n_o \left[|x_m - x_n| < \varepsilon\right] \Longrightarrow$$
$$\forall \tau(m), \tau(n) \geq \tau(n_o) \left[|x_{\tau(m)} - x_{\tau(n)}| < \varepsilon\right] \Longrightarrow$$
$$\forall\, m,n \geq n_o \left[|y_m - y_n| < \varepsilon\right],$$

wobei benutzt wird, daß $\tau(n) \geq n$ für alle $n \in \mathbb{N}_o$ gilt.

b) Zu $\varepsilon > 0$ existiert ein n_o mit

$$\forall\, m,n \geq n_o \left[|x_m - x_n| < \varepsilon\right] \Longrightarrow$$
$$\forall\, n \geq n_o \left[|x_n - x_{\tau(n)}| = |x_n - y_n| < \varepsilon\right] \Longrightarrow$$

$(x_n - y_n) \in N(K)$. //

4.1.6 HILFSSATZ:
Sind $(x_n) \in C(K)$ und $(\varepsilon_n) \in N(K)$ mit $\varepsilon_n > 0$ für alle $n \in \mathbb{N}_o$, dann existiert eine Teilfolge (z_n) von (x_n), so daß gilt:

$$\forall\, n \in \mathbb{N}_o\ \forall\, k,l \geq n \left[|z_k - z_l| < \varepsilon_n\right].$$

Bemerkung: Ist K der Körper der rationalen Zahlen, so kann $\varepsilon_n := \frac{1}{n+1}$ gewählt werden.

Beweis: Induktive Bestimmung der $\tau(n) \in \mathbb{N}_o$ mit folgenden Eigenschaften:

(i) Für $m < n$ gilt $\tau(m) < \tau(n)$;

(ii) $\forall\, n \in \mathbb{N}_o\ \forall\, k,l \geq \tau(n) \left[|x_k - x_l| < \varepsilon_n\right]$.

Beginn $n = 0$: Zu ε_o sei $n_o \in \mathbb{N}_o$ mit $\forall\, k,l \geq n_o \left[|x_n - x_l| < \varepsilon_o\right]$ gewählt. Setze $\tau(0) := n_o$.
Schluß von n auf $n+1$: Seien schon $\tau(0),\ldots,\tau(n)$ so bestimmt, daß dafür (i) und (ii) gelten. Zu ε_{n+1} gibt es dann ein $r_o \in \mathbb{N}_o$ mit $\forall\, k,l \geq r_o \left[|x_k - x_l| < \varepsilon_{n+1}\right]$. Setze $\tau(n+1) := \max(r_o, \tau(n) + 1)$, dann gelten (i) und (ii) für $\tau(n+1)$. Damit ist $\tau\colon \mathbb{N}_o \longrightarrow \mathbb{N}_o$ definiert. Setzt man nun $z_n := x_{\tau(n)}$ für alle $n \in \mathbb{N}_o$, so ist (z_n) wegen (i) eine Teilfolge von (x_n) und wegen (i) und (ii) folgt die Behauptung. //

4.2 Der Körper der reellen Zahlen

Zunächst zeigen wir für einen beliebigen angeordneten Körper K, daß $C(K)$ in naheliegender Weise zu einem Ring gemacht werden kann.

4.2.1 SATZ:
Sei K ein angeordneter Körper und $C(K)$ die Menge der Cauchy-Folgen in K. Dann ist $C(K)$ mit der Addition $(x_n) + (y_n) := (x_n + y_n)$ und der Multiplikation $(x_n) \cdot (y_n) := (x_n \cdot y_n)$ ein kommutativer Ring mit Einselement. Das Einselement ist die Folge (x_n) mit $x_n = 1$ für alle $n \in \mathbb{N}_o$.

Beweis: 1) Mit (x_n) und (y_n) ist auch $(x_n + y_n)$ eine Cauchy-Folge. Sei nämlich $\varepsilon > 0$, $\varepsilon \in K$. Dann gibt es ein $n_1 \in \mathbb{N}_o$, so daß für alle $m,n \geq n_1$ gilt $|x_m - x_n| < \frac{\varepsilon}{2}$. Ebenso gibt es ein $n_2 \in \mathbb{N}_o$, so daß für alle $m,n \geq n_2$ gilt $|y_m - y_n| < \frac{\varepsilon}{2}$. Für alle $m,n \geq n_o := \max(n_1,n_2)$ ist dann

$$|(x_m + y_m) - (x_n + y_n)| \leq |x_m - x_n| + |y_m - y_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon .$$

2) Mit (x_n) und (y_n) ist auch $(x_n y_n)$ eine Cauchy-Folge. Sei nämlich $\varepsilon > 0$, $\varepsilon \in K$. Seien weiter $|x_n| \leq z_1$, $|y_n| \leq z_2$ für alle $n \in \mathbb{N}_o$ und $z := \max(z_1,z_2,1)$. Dann gibt es ein $n_o \in \mathbb{N}_o$, so daß für alle $m,n \geq n_o$ gilt $|x_m - x_n| < \frac{\varepsilon}{2z}$ und $|y_m - y_n| < \frac{\varepsilon}{2z}$. Daraus folgt

$$\begin{aligned} |x_m y_m - x_n y_n| &= |x_m y_m - x_m y_n + x_m y_n - x_n y_n| \\ &\leq |x_m||y_m - y_n| + |x_m - x_n||y_n| \\ &< 2z\frac{\varepsilon}{2z} = \varepsilon . \end{aligned}$$

3) Die Folge (x_n) mit $x_n = 1$ für alle $n \in \mathbb{N}_o$ ist trivialerweise das Einselement der Multiplikation.

4) Die Ringeigenschaften lassen sich jetzt durch komponentenweise Rechnungen leicht nachprüfen, wie z.B. die Kommutativität der Addition:
$(x_n) + (y_n) = (x_n + y_n) = (y_n + x_n) = (y_n) + (x_n)$. //

4.2.2 SATZ:
Die Menge der Nullfolgen $N(K)$ ist ein Ideal in $C(K)$.

Beweis: 1) Seien (x_n) und (y_n) Nullfolgen. Dann ist auch $(x_n)+(y_n)$ eine Nullfolge. Für $\varepsilon > 0$ gibt es nämlich ein $n_o \in \mathbb{N}_o$, so daß für alle $n \geq n_o$ gilt: $|x_n| < \frac{\varepsilon}{2}$ und $|y_n| < \frac{\varepsilon}{2}$. Dann ist $|x_n + y_n| \leq |x_n| + |y_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$.

2) Sei $(x_n) \in C(K)$ und $(y_n) \in N(K)$. Dann ist $(x_n)(y_n) \in N(K)$. Sei nämlich $\varepsilon > 0$. Es gibt ein $z > 0$ mit $|x_n| < z$ für alle $n \in \mathbb{N}_o$. Weiter gibt es ein $n_o \in \mathbb{N}_o$ mit $|y_n| < \frac{\varepsilon}{z}$ für alle $n \geq n_o$. Dann gilt $|x_n y_n| = |x_n||y_n| < z \cdot \frac{\varepsilon}{z} = \varepsilon$ für alle $n \geq n_o$. //

Nachdem wir wissen, daß die Menge $N(K)$ der Nullfolgen ein Ideal in $C(K)$ ist, kann der Restklassenring $C(K)/N(K)$ (im Sinne von III.3.3.2) betrachtet werden. Ist $(x_n) \in C(K)$, so bezeichne

$$(\overline{x_n}) := (x_n) + N(K) \in C(K)/N(K)$$

die durch (x_n) erzeugte Restklasse modulo $N(K)$. Sei auch $(y_n) \in C(K)$. Genau dann gilt $(\overline{x_n}) = (\overline{y_n})$, wenn $(x_n) - (y_n) = (x_n - y_n) \in N(K)$ (siehe IV.2.4.2).

Das Ziel der weiteren Überlegungen ist es zu zeigen, daß $C(K)/N(K)$ ein Körper ist.

4.2.3 SATZ:
$C(K)/N(K)$ ist ein Körper.

Beweis: Nach III.3.8 ist $C(K)/N(K)$ ein kommutativer Ring mit dem Einselement $(\overline{e_n}) = (e_n) + N(K)$ mit $e_n = 1$ für alle $n \in \mathbb{N}_o$. Es bleibt zu zeigen, daß zu einem beliebigen Element $(\overline{x_n}) = (x_n) + N(K) \in C(K)/N(K)$ mit $(\overline{x_n}) \neq 0$ ein inverses Element existiert, d.h. zu $(x_n) \in C(K) \setminus N(K)$ ist ein $(y_n) \in C(K)$ anzugeben, so daß $(x_n y_n - 1) \in N(K)$ gilt. Da (x_n) keine Nullfolge ist, existiert nach 4.1.3 ein k_o, so daß $x_n \neq 0$ für alle $n \geq k_o$ gilt. Wir definieren (y_n) durch $y_n := x_n^{-1}$ für alle $n \geq k_o$ und $y_n := 1$ für alle $n < k_o$. Für alle $n \geq k_o$ gilt dann $x_n y_n = 1$, also

$x_n y_n - 1 = 0$, folglich ist $(x_n y_n - 1)$ eine Nullfolge. Es gilt also $(\overline{x_n})(\overline{y_n}) = (\overline{x_n y_n}) = (\overline{e_n})$.

Zu zeigen bleibt, daß (y_n) eine Cauchy-Folge ist. Zunächst ist im Sinne von 4.1.3 $|x_n| > \delta$ für alle $n \geq k_o$. Ist nun $\varepsilon > 0$ gegeben, dann existiert ein $n_o \geq k_o$, so daß für alle $m,n \geq n_o$

$$|x_m - x_n| < \varepsilon\delta^2$$

gilt. Es folgt

$$|y_m - y_n| = \left|\frac{x_n - x_m}{x_m x_n}\right| < \frac{\varepsilon\delta^2}{\delta^2} = \varepsilon .$$

Also gilt tatsächlich $(y_n) \in C(K)$. //

Die Cauchy-Folge (x_n) mit $x_n = x$ für alle $n \in \mathbb{N}_o$ nennen wir k o n s t a n t e F o l g e und schreiben dafür im folgenden auch (x) und entsprechend $(\overline{x})$ $= (x) + N(K)$. Da unter den konstanten Folgen offensichtlich nur die Folge (0) eine Nullfolge ist, gilt: $(\overline{x}) = (\overline{y}) \Longleftrightarrow x = y$.

Man prüft nun leicht nach, daß die Abbildung

$$\varphi: K \ni x \longmapsto (\overline{x}) \in C(K)/N(K)$$

ein injektiver Ringhomomorphismus ist. Daher ist $Bi(\varphi) = \varphi(K)$ ein Unterkörper von $C(K)/N(K)$. Oft wird $\varphi(K)$ mit K identifiziert und für das Element $(\overline{x})$ wieder x geschrieben. Durch diese Identifizierung wird $C(K)/N(K)$ zu einem Oberkörper von K selbst. Um Unklarheiten zu vermeiden, machen wir von dieser Identifizierung vorläufig keinen Gebrauch.

Wichtig für das Verständnis der weiteren Überlegungen ist die folgende einfache Feststellung. Für $x \in K$ und $(x_n) \in C(K)$ gilt: $(\overline{x}) = (\overline{x_n}) \Longleftrightarrow x = \lim(x_n)$.
Beweis: $x = \lim(x_n) \Longleftrightarrow 0 = \lim(x - x_n) \Longleftrightarrow (x - x_n) \in N(K)$ $\Longleftrightarrow (\overline{x}) = (\overline{x_n})$.

Mit anderen Worten besagt dies: genau dann besitzt die Cauchy-Folge (x_n) einen Limes $x \in K$, wenn $(\overline{x_n}) \in \varphi(K)$ gilt. Daraus folgt ferner: Jede Cauchy-Folge besitzt einen Limes in K , wenn $\varphi(K) = C(K)/N(K)$ gilt.

4.2.4 DEFINITION:
Für $K = \mathbb{Q}$ heißt $\mathbb{R} := C(\mathbb{Q})/N(\mathbb{Q})$ Körper der r e e l l e n Z a h l e n .

Da es irrationale reelle Zahlen gibt, ist $\mathbb{R}$ echter Oberkörper von $\varphi(\mathbb{Q})$ bzw. (nach Identifizierung) von $\mathbb{Q}$. Wesentlich für $\mathbb{R}$ ist die Tatsache, daß $\varphi(\mathbb{R}) = C(\mathbb{R})/N(\mathbb{R})$ gilt, d.h. daß jede Cauchy-Folge von reellen Zahlen einen Limes in $\mathbb{R}$ besitzt. Diese Eigenschaft von $\mathbb{R}$ heißt V o l l s t ä n d i g k e i t s - e i g e n s c h a f t von $\mathbb{R}$. Sie ist für die Analysis grundlegend. Ihr Beweis ist das Hauptziel der weiteren Überlegungen.

Um an den Gesichtspunkt aus der Einleitung anzuknüpfen, weisen wir darauf hin, daß jetzt jeder unendliche Dezimalbruch als Element von $\mathbb{R}$ aufgefaßt werden kann, indem man ihn als Folge von rationalen Zahlen betrachtet. Ist der Dezimalbruch $a,a_1a_2a_3\ldots$ (wobei $a_i \in \{0,1,\ldots,9\}$), dann ist die fragliche Folge (x_n) mit $x_n := a,a_1a_2\ldots a_n$. Jede solche Folge ist eine Cauchy-Folge und bestimmt daher ein Element $(\overline{x_n})$ in $C(\mathbb{Q})/N(\mathbb{Q})$. Jetzt kann man auch bereits einsehen, warum die reellen Zahlen $3,0000\ldots$ und $2,9999\ldots$ gleich sind: Die zugehörigen Cauchy-Folgen erzeugen die gleiche Restklasse modulo $N(\mathbb{Q})$.

Umgekehrt kann man auch jeder reellen Zahl $(\overline{x_n})$ einen unendlichen Dezimalbruch zuordnen. Diese Zuordnung, die einer speziellen Konstruktion bedarf, um die rationalen Zahlen in geeigneter Weise in endliche oder unendliche Dezimalbrüche umzuwandeln, soll hier nicht durchgeführt werden. Andere wichtige Eigenschaften von $\mathbb{R}$ werden wir wieder für $C(K)/N(K)$ mit einem beliebigen angeordneten Körper K untersuchen.

4.3 Ordnung und absoluter Betrag von C(K)/N(K)

Zunächst wollen wir für einen beliebigen angeordneten Körper mit Hilfe der Ordnung von K eine Ordnung von $C(K)/N(K)$ definieren.

4.3.1 DEFINITION:
Seien $(\overline{x_n}),(\overline{y_n}) \in C(K)/N(K)$.

(1) $(\overline{x_n}) \leq (\overline{y_n}) :\Longleftrightarrow \forall\, \varepsilon > 0,\ \varepsilon \in K\ \exists\, n_o \in \mathbb{N}_o\ \forall\, n \geq n_o,\ n \in \mathbb{N}_o\ \left[x_n < y_n + \varepsilon\right]$,

(2) $(\overline{x_n}) < (\overline{y_n}) :\Longleftrightarrow (\overline{x_n}) \leq (\overline{y_n}) \wedge (\overline{x_n}) \neq (\overline{y_n})$.

4.3.2 FOLGERUNG:
Seien $(x_n),(y_n) \in C(K)/N(K)$. Dann gilt:

$(\overline{x_n}) < (\overline{y_n}) \Longleftrightarrow \exists \delta > 0,\ \delta \in K\ \exists\, k_o \in \mathbb{N}_o\ \forall\, n \geq n_o,\ n \in \mathbb{N}_o\ \left[x_n + \delta < y_n\right]$.

Beweis: "$\Longrightarrow$": Wegen $(\overline{x_n}) \neq (\overline{y_n})$ ist $(x_n - y_n)$ keine Nullfolge, so daß dafür 4.1.3 gilt. Es fragt sich nur, welcher Fall in 4.1.3 vorliegt. Wegen (1) gilt $x_n < y_n + \varepsilon$ für beliebige $\varepsilon > 0$ und alle hinreichend großen n . Also kann nicht $y_n + \delta < x_n$ $(\Longleftrightarrow x_n - y_n > \delta)$ für ein $\delta > 0$ und alle $n \geq k_o$ gelten. Daher liegt in 4.1.3 der zweite Fall, d.h. $x_n + \delta < y_n$ für $\delta > 0$ und alle $n \geq k_o$ vor.

"$\Longleftarrow$": Aus $x_n + \delta < y_n$ für alle $n \geq k_o$ folgt $x_n < y_n - \delta < y_n < y_n + \varepsilon$ für jedes $\varepsilon > 0$ und alle $n \geq k_o$, also gilt $(\overline{x_n}) \leq (\overline{y_n})$. Wegen $y_n - x_n > \delta$ für alle $n \geq k_o$ ist $(y_n - x_n)$ keine Nullfolge, also gilt $(\overline{x_n}) \neq (\overline{y_n})$. //

4.3.3 SATZ:
$C(K)/N(K)$ ist bei der in 4.3.1 definierten Relation $\leq$ ein angeordneter Körper. Bei dieser Ordnung gilt für Elemente aus $\varphi(K)$:

$$(\overline{x}) \leq (\overline{y}) \Longleftrightarrow x \leq y ,$$

wobei $x \leq y$ die Ordnung in K bezeichnet.

Bemerkung: Wegen der letzten Eigenschaft sagt man, daß die Ordnung von $C(K)/N(K)$ die Ordnung von K fortsetzt.

Beweis: 1) Zunächst ist zu zeigen, daß die gegebene Definition der Ordnung unabhängig von der erfolgten Auswahl der Repräsentanten von $(\overline{x_n})$ bzw. $(\overline{y_n})$ ist. Seien (x_n) und (x_n') Repräsentanten für $(\overline{x_n})$ und (y_n) und (y_n') für $(\overline{y_n})$. Für (x_n) und (y_n) gelte die Bedingung der Definition in 4.3.1. Zu $\varepsilon > 0$, $\varepsilon \in K$ gibt es dann $n_0 \in \mathbb{N}_0$, so daß für alle $n \in \mathbb{N}_0$ mit $n \geq n_0$ gilt $x_n - y_n < \frac{\varepsilon}{3}$. Weiter gibt es ein $n_1 \in \mathbb{N}_0$, so daß für alle $n \geq n_1$ gilt $|x_n - x_n'| < \frac{\varepsilon}{3}$, und es gibt ein $n_2 \in \mathbb{N}_0$, so daß für alle $n \geq n_2$ gilt $|y_n - y_n'| < \frac{\varepsilon}{3}$. Für $n_3 := \max(n_0, n_1, n_2)$ und alle $n \geq n_3$ gilt dann

$$x_n' - y_n' = (x_n' - x_n) + (x_n - y_n) + (y_n - y_n') < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon .$$

Also gilt die Bedingung der Definition auch für (x_n') und (y_n').

2) Für $(\overline{x_n})$, $(\overline{y_n})$ ist zu zeigen: Es gilt genau eine der Beziehungen:

$$(\overline{x_n}) < (\overline{y_n}) \ , \ (\overline{x_n}) = (\overline{y_n}) \ , \ (\overline{y_n}) < (\overline{x_n}) .$$

Wir nehmen an, daß $(\overline{x_n}) \neq (\overline{y_n})$ gilt. Aus 4.1.3 und 4.3.2 folgt dann, daß entweder $(\overline{x_n}) < (\overline{y_n})$ oder $(\overline{y_n}) < (\overline{x_n})$ (im ausschließenden Sinne) gilt.

3) Da sich die Bedingungen in 2) gegenseitig ausschließen, gilt auch:

$$(\overline{x_n}) \leq (\overline{y_n}) \wedge (\overline{y_n}) \leq (\overline{x_n}) \Longleftrightarrow (\overline{x_n}) = (\overline{y_n})$$

(Antisymmetrie).

4) Gelte $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{y_n}) \leq (\overline{z_n})$. Wenn in einem oder beiden Fällen die Gleichheit steht, dann ist $(\overline{x_n}) \leq (\overline{z_n})$. Gilt aber $(\overline{x_n}) < (\overline{y_n})$ und $(\overline{y_n}) < (\overline{z_n})$, so existieren nach 4.3.2 $\delta_1, \delta_2 > 0$ und $k_1, k_2 \in \mathbb{N}_0$, so daß $y_n - x_n > \delta_1$ für alle $n \geq k_1$ und $z_n - y_n > \delta_2$

für alle $n \geq k_2$ gilt. Mit $\delta_o := \delta_1 + \delta_2$ und $k_o := \max(k_1, k_2)$ folgt dann $z_n - x_n = z_n - y_n + y_n + x_n > \delta_o$ für alle $n \geq k_o$. Also gilt $(\overline{x_n}) \leq (\overline{z_n})$.

5) Wir stellen nun fest, daß die gegebene Ordnung die Ordnung von K fortsetzt. Für $x, y \in K$ gilt zunächst

$$x < y \iff y - x > \frac{1}{2}(y - x) > 0 .$$

Auf Grund von 4.3.2 mit $k_o = 0$ und $\delta := \frac{1}{2}(y - x)$ ist dies äquivalent mit $(\overline{x}) < (\overline{y})$. Da wegen der Injektivität der Abbildung φ auch

$$x = y \iff (\overline{x}) = (\overline{y})$$

gilt, folgt insgesamt

$$x \leq y \iff (\overline{x}) \leq (\overline{y}) .$$

6) Es bleiben die Monotoniegesetze zu zeigen. Seien $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{z_n}) \in C(K)/N(K)$ gegeben. Nach Definition der Ordnung gibt es zu jedem $\varepsilon > 0$ ein $n_o \in \mathbb{N}_o$, so daß $x_n - y_n < \varepsilon$ für alle $n \geq n_o$ gilt. Dann folgt $(x_n + z_n) - (y_n + z_n) < \varepsilon$, also gilt $(\overline{x_n}) + (\overline{z_n}) = (\overline{x_n + z_n}) \leq (\overline{y_n + z_n}) = (\overline{y_n}) + (\overline{z_n})$.

7) Seien jetzt $(\overline{x_n}) \leq (\overline{y_n})$ und $0 \leq (\overline{z_n})$ gegeben. Zu zeigen ist $(\overline{x_n})(\overline{z_n}) \leq (\overline{y_n})(\overline{z_n})$. Gilt $(\overline{x_n}) = (\overline{y_n})$ oder $0 = (\overline{z_n})$, dann ist die Behauptung erfüllt. Sei daher $(\overline{x_n}) < (\overline{y_n})$ und $0 = (\overline{0}) < (\overline{z_n})$, dann existieren nach 4.3.2 $\delta_1, \delta_2 > 0$ und $k_1, k_2 \in \mathbb{N}_o$ mit

$$y_n - x_n > \delta_1 \quad \text{für} \quad n \geq k_1 , \qquad z_n > \delta_2 \quad \text{für} \quad n \geq k_2 .$$

Daraus folgt für alle $n \geq k_o := \max(k_1, k_2)$

$$(y_n - x_n) z_n = y_n z_n - x_n z_n > \delta_1 \delta_2 ,$$

also gilt $(\overline{x_n z_n}) = (\overline{x_n})(\overline{z_n}) < (\overline{y_n z_n}) = (\overline{y_n})(\overline{z_n})$. //

Nach diesem Satz überträgt sich die Ordnung von K bei dem Körperisomorphismus φ auf $\varphi(K)$, d.h. $x \leq y \iff \varphi(x) \leq \varphi(y)$. Man sagt daher auch, daß K und $\varphi(K)$ o r d n u n g s i s o m o r p h sind *).

*) Siehe ordnungstreue Abbildungen VI.2.1.2.

Nach Definition der Cauchy-Folge ergibt sich unmittelbar, daß (x_n) genau dann eine Cauchy-Folge von K ist, wenn $(\varphi(x_n))$ eine Cauchy-Folge von $\varphi(K)$ ist. Davon wird im folgenden ohne besonderen Hinweis Gebrauch gemacht.

4.3.4 SATZ:
Seien $(\overline{x_n}), (\overline{y_n}) \in C(K)/N(K)$ mit $(\overline{x_n}) < (\overline{y_n})$ gegeben. Dann existiert ein $z \in K$ mit $(\overline{x_n}) < (\overline{z}) < (\overline{y_n})$. Man sagt daher auch, daß $\varphi(K)$ (bzw. bei Identifizierung K selbst) dichte Teilmenge von $C(K)/N(K)$ ist.

Beweis: Gelte im Sinne von 4.3.2

$$y_n - x_n > \delta \quad \text{für alle} \quad n \geq k_o .$$

Sei $\varepsilon := \frac{1}{4}\delta$, dann existiert ein $n_o \geq k_o$, so daß für alle $n \geq n_o$

$$|x_n - x_{n_o}| < \varepsilon \quad , \quad |y_n - y_{n_o}| < \varepsilon$$

gilt. Sei $z := x_{n_o} + 2\varepsilon$, dann gilt für alle $n \geq n_o$

$$z - x_n = x_{n_o} + 2\varepsilon - x_n > 2\varepsilon - \varepsilon = \varepsilon$$

$$y_n - z = y_n - y_{n_o} + y_{n_o} - x_{n_o} - 2\varepsilon > -\varepsilon + \delta - 2\varepsilon = \delta - 3\varepsilon = \varepsilon .$$

Nach 4.3.2 folgt daraus $(\overline{x_n}) < (\overline{z}) < (\overline{y_n})$. //

Für den angeordneten Körper $C(K)/N(K)$ kann im Sinne von 3.3 der absolute Betrag definiert werden. Dafür erhält man aus 4.3.4 unmittelbar die folgende Aussage.

4.3.5 FOLGERUNG:
Zu $(\overline{x_n}), (\overline{y_n}), (\overline{\varepsilon_n}) \in C(K)/N(K)$ mit $|(\overline{x_n}) - (\overline{y_n})| < (\overline{\varepsilon_n})$ gibt es ein $\varepsilon \in K$ mit $|(\overline{x_n}) - (\overline{y_n})| < (\overline{\varepsilon}) < (\overline{\varepsilon_n})$. //

Für spätere Anwendungen stellen wir noch fest, was $|(\overline{x_n}) - (\overline{y_n})| < (\overline{\varepsilon})$ bedeutet.

4.3.6 BEMERKUNG:
$|(\overline{x_n}) - (\overline{y_n})| < (\overline{\varepsilon})$ gilt genau dann, wenn ein $k_o \in \mathbb{N}_o$

und ein $\delta > 0$, $\delta \in K$ so existieren, daß
$|x_n - y_n| < \varepsilon - \delta$ für alle $n \geq k_o$ gilt.

Beweis: $|(\overline{x_n}) - (\overline{y_n})| < (\overline{\varepsilon})$ gilt genau dann, wenn $(\overline{x_n}) - (\overline{y_n}) = (\overline{x_n - y_n}) < (\overline{\varepsilon})$ und $(\overline{y_n}) - (\overline{x_n}) = (\overline{y_n - x_n}) < (\overline{\varepsilon})$ gelten. Nach 4.3.2 ist dies genau dann der Fall, wenn $\delta_1 > 0$, $\delta_2 > 0$, $\delta_1, \delta_2 \in K$ sowie $k_1, k_2 \in \mathbb{N}_o$ so existieren, daß

$$(x_n - y_n) + \delta_1 < \varepsilon \quad \text{für alle} \quad n \geq k_1$$

und

$$(y_n - x_n) + \delta_2 < \varepsilon \quad \text{für alle} \quad n \geq k_2$$

gelten. Für $\delta := \min(\delta_1, \delta_2)$ und $k_o := \max(k_1, k_2)$ folgt

$$|x_n - y_n| < \varepsilon - \delta_o \quad \text{für alle} \quad n \geq k_o .$$

Umgekehrt folgen hieraus die vorhergehenden Ungleichungen mit $\delta_1 = \delta_2 = \delta_o$ und $k_1 = k_2 = k_o$. //

4.4 Vollständigkeit

Unser Ziel ist es, einen Oberkörper von K zu konstruieren, in dem jede Cauchy-Folge einen Grenzwert besitzt. An Stelle von K lösen wir diese Aufgabe für den zu K ordnungsisomorphen Körper $\varphi(K)$ (bzw. bei Identifizierung von K mit $\varphi(K)$ für K selbst). Die Cauchy-Folgen aus $\varphi(K)$ sind von der Form $(\varphi(x_n))$, wobei (x_n) eine Cauchy-Folge aus K ist. Wir stellen zunächst fest, daß $(\varphi(x_n))$ in $L := C(K)/N(K)$ den Grenzwert $(\overline{x_n})$ besitzt. Das ist nach Definition von L nicht überraschend, denn wir hatten L genau in diesem Sinne konstruiert. Überraschend ist jedoch, daß jede Cauchy-Folge aus L (und nicht nur aus dem Unterkörper $\varphi(K)$ von L) in L einen Grenzwert besitzt.

4.4.1 DEFINITION:
Ein angeordneter Körper L heißt **vollständig** :$\Longleftrightarrow$ Jede Cauchy-Folge aus L besitzt einen Grenz-

wert in L .

4.4.2 SATZ:
Sei $(x_n) \in C(K)$. Dann hat $(\varphi(x_n))$ in $C(K)/N(K)$ den Grenzwert $(\overline{x_n})$.

Beweis: Es ist zu zeigen: Zu jedem $(\overline{\varepsilon_n}) \in C(K)/N(K)$ mit $(\overline{\varepsilon_n}) > 0 \; (= (\overline{0}))$ existiert ein $n_o \in \mathbb{N}_o$, so daß für alle $m \geq n_o$

$$|\varphi(x_m) - (\overline{x_n})| < (\overline{\varepsilon_n})$$

gilt. Beachte dabei, daß $\varphi(x_m)$ die Restklasse zur konstanten Folge mit dem (konstanten) Folgenglied x_m ist. Nach 4.3.5 existiert zu $(\overline{\varepsilon_n}) > 0$ ein $\varepsilon \in K$ mit $0 < (\overline{\varepsilon}) < (\overline{\varepsilon_n})$. Aus $0 < (\overline{\varepsilon})$ folgt $0 < \varepsilon$ (nach 4.3.2). Wegen $(x_n) \in C(K)$ existiert ein k_o , so daß für alle $m,n \geq k_o$

$$|x_m - x_n| < \frac{\varepsilon}{2} = \varepsilon - \frac{\varepsilon}{2}$$

gilt. Setzt man in 4.3.6 $\delta := \frac{\varepsilon}{2}$, so folgt aus 4.3.6 für alle $m = k_o$

$$|(x_m) - (\overline{x_n})| < (\overline{\varepsilon}) < (\overline{\varepsilon_n}) \; ,$$

was zu zeigen war. //

4.4.3 SATZ:
$L := C(K)/N(K)$ ist vollständig.

Beweis: Wir unterscheiden zwei Fälle. Zunächst nehmen wir an, daß jede Nullfolge (x_n) in K konstant wird, d.h. es gibt ein $n_o \in \mathbb{N}_o$ mit $x_n = 0$ für alle $n \geq n_o$. Sei $(y_n) \in C(K)$. Dann gilt: $(y_{n+1} - y_n)$ ist eine Nullfolge wegen 4.1.5.b), also gibt es ein $n_o \in \mathbb{N}_o$, so daß für alle $n \geq n_o$ gilt $y_{n+1} - y_n = 0$, d.h. $y_n = y_{n_o}$. Daraus folgt $(\overline{y_n}) = (\overline{y_{n_o}})$, d.h. $\varphi: K \longrightarrow C(K)/N(K)$ ist ein Isomorphismus. Wegen 4.4.2 ist daher $C(K)/N(K)$ vollständig.

Wir können nun annehmen, daß es eine Nullfolge (x_n) gibt, für die unendlich viele $x_n \neq 0$ sind. Sei (x'_n) die Teilfolge der von Null verschiedenen Ele-

mente von (x_n) und sei $(\varepsilon_n) := (|x'_n|)$. Dann ist $(\varepsilon_n) \in N(K)$ und es gilt $\varepsilon_n > 0$ für alle $n \in \mathbb{N}_o$. Für diese Nullfolge steht Hilfssatz 4.1.6 zur Verfügung, von dem wir im folgenden Gebrauch machen.

Sei (y_i) eine Cauchy-Folge in L mit $y_i = (\overline{x_{i,n}})$, wobei also $(x_{i,n})$ für jedes $i \in \mathbb{N}_o$ eine Cauchy-Folge in K ist. Den Grenzwert von (y_i) konstruieren wir durch ein "Diagonalverfahren".

Zunächst werden die Repräsentanten $(x_{i,n})$ von y_i , $i \in \mathbb{N}_o$ durch Repräsentanten ersetzt, die für ein solches Diagonalverfahren geeignet sind. Sei im Sinne von 4.1.6 $(z_{i,n})$ eine Teilfolge von $(x_{i,n})$, dann gilt wegen 4.1.5

$$y_i = (\overline{x_{i,n}}) = (\overline{z_{i,n}}) .$$

Man beachte, daß in $(z_{i,n})$ der Index i fest ist und der Folgenindex n ist.

Wir bilden nun zu der Folge von Folgen

$$(z_{o,n}), (z_{1,n}), (z_{2,n}), \ldots$$

die Diagonalfolge

$$(z_{o,o}, z_{1,1}, z_{2,2}, z_{3,3}, \ldots)$$

und behaupten:

(1) $(z_{n,n}) \in C(K)$

(2) $\lim\limits_{i \in \mathbb{N}_o} (y_i) = (\overline{z_{n,n}})$.

Den Beweis für (1) und (2) führen wir in drei Schritten.

1. Schritt: Behauptung: Zu $\varepsilon > 0$, $\varepsilon \in K$ existiert ein n_o , so daß für alle $i,j,m,n \geq n_o$

(3) $|z_{i,m} - z_{j,n}| < \frac{3}{4} \varepsilon$

gilt.

Sei $n_1 \in \mathbb{N}_o$ so groß, daß $\varepsilon_{n_1} < \frac{1}{4} \varepsilon$ gilt. Dann folgt nach 4.1.6, daß für alle $i,j \in \mathbb{N}_o$ und alle $l,m,n \geq n_1$

$$|z_{i,m} - z_{i,l}| < \frac{1}{4}\varepsilon\,, \quad |z_{j,l} - z_{j,n}| < \frac{1}{4}\varepsilon$$

gilt.

Da (y_i) eine Cauchy-Folge ist, gibt es zu $\varepsilon > 0$, $\varepsilon \in K$ ein $n_2 \in \mathbb{N}_o$, so daß für alle $i,j \geq n_2$

$$|y_i - y_j| = |(\overline{z_{i,n}}) - (\overline{z_{j,n}})| < (\overline{\frac{\varepsilon}{4}})$$

gilt.

Nach 4.3.6 existiert dann ein $n_3 \in \mathbb{N}_o$, so daß für alle $l \geq n_3$

$$|z_{i,l} - z_{j,l}| < \frac{1}{4}\varepsilon$$

gilt. Dabei kann n_3 von i und j abhängen. Für $n_o := \max(n_1,n_2)$ und alle $i,j,m,n \geq n_o$ und alle $l \geq \max(n_1,n_3)$ folgt dann

$$|z_{i,m} - z_{j,n}| \leq |z_{i,m} - z_{i,l}| + |z_{i,l} - z_{j,l}| + |z_{j,l} - z_{j,n}| < \frac{3}{4}\varepsilon\,.$$

2. Schritt: Für $i = m$ und $j = n$ folgt aus (3)

$$|z_{m,m} - z_{n,n}| < \frac{3}{4}\varepsilon < \varepsilon$$

für alle $m,n \geq n_o$. Das besagt, daß $(z_{n,n}) \in C(K)$, d.h. (1) gilt.

3. Schritt: Für $j = m = n$ erhält man aus (3)

$$|z_{i,n} - z_{n,n}| < \frac{3}{4}\varepsilon = \varepsilon - \frac{1}{4}\varepsilon$$

für alle $i,n \geq n_o$. Nach 4.3.6 folgt

$$|(\overline{z_{i,n}}) - (\overline{z_{n,n}})| = |y_i - (\overline{z_{n,n}})| < (\overline{\varepsilon})$$

für alle $i \geq n_o$. Daraus folgt wegen 4.3.5

$$\lim_{i \in \mathbb{N}_o} (y_i) = (\overline{z_{n,n}})\,,$$

d.h. es gilt auch (2), womit alles bewiesen ist. //

Im Falle $K = \mathbb{Q}$ liefert dieser Satz die Vollständigkeit des Körpers $\mathbb{R} = C(\mathbb{Q})/N(\mathbb{Q})$ der reellen Zahlen.

Zum Schluß dieses Abschnitts wollen wir noch eine Eigenschaft der reellen Zahlen beweisen, die zur Vollständigkeit äquivalent ist und die daher auch

zur Definition der Vollständigkeit benutzt werden kann.

4.4.3 SATZ:
Jede nicht-leere nach oben beschränkte Menge $M \subset \mathbb{R}$ besitzt ein Supremum und jede nicht-leere nach unten beschränkte Menge $M \subset \mathbb{R}$ besitzt ein Infimum.

Beweis: Beim Beweis werden wir $\mathbb{Q}$ mit $\varphi(\mathbb{Q})$ identifizieren. Wir führen den Beweis zunächst für den ersten Fall. Sei also $M \neq \emptyset$ und M nach oben beschränkt. Der Beweis erfolgt durch Intervallschachtelung. Induktiv werden zwei Folgen rationaler Zahlen (a_n) und (b_n) mit folgenden Eigenschaften definiert:

(i) $a_n < b_n$

(ii) $\{x \mid x \in M \wedge a_n < x \leq b_n\} \neq \emptyset$

(iii) b_n ist obere Schranke von M, d.h. $\forall\, x \in M [x \leq b_n]$

(iv) $b_n - a_n = \frac{1}{2^n}(b_o - a_o)$.

Induktionsbeginn: Sei $a_o := x_o - 1$ für ein $x_o \in M$ und sei b_o eine beliebige obere Schranke von M. Dann sind dafür (i) bis (iv) offensichtlich erfüllt.

Seien schon $a_o, \ldots, a_n$ und $b_o, \ldots, b_n$ mit (i) bis (iv) bestimmt.

Induktionsschluß: Ist $\frac{1}{2}(a_n + b_n)$ eine obere Schranke von M, dann setze man

$$a_{n+1} := a_n \ , \quad b_{n+1} := \frac{1}{2}(a_n + b_n) \ .$$

Ist $\frac{1}{2}(a_n + b_n)$ keine obere Schranke von M, dann setze man

$$a_{n+1} := \frac{1}{2}(a_n + b_n) \ , \quad b_{n+1} := b_n \ .$$

Offensichtlich gelten dann (i), (ii), (iii) für a_{n+1} und b_{n+1}. Ferner folgt nach Induktionsannahme

$$b_{n+1} - a_{n+1} = \frac{1}{2}(b_n - a_n) = \frac{1}{2^{n+1}}(b_0 - a_0) \ .$$

Wegen $a_m \leq a_{m+i} < b_{m+i} \leq b_m$ für alle $i \in \mathbb{N}_0$ folgt für $n \geq m$

$$|a_n - a_m| = a_n - a_m < b_m - a_m = \frac{1}{2^m}(b_0 - a_0) \ .$$

Daraus ergibt sich sofort, daß (a_n) eine Cauchy-Folge ist. Ebenso gilt für $n \geq m$

$$|b_m - b_n| = b_m - b_n < b_m - a_m = \frac{1}{2^m}(b_0 - a_0)$$

und folglich ist auch (b_n) eine Cauchy-Folge. Wegen $b_n - a_n = 2^{-n}(b_0 - a_0)$ ist $(b_n - a_n)$ eine Nullfolge, also gilt $(\overline{a_n}) = (\overline{b_n})$.

Behauptung: $s := (\overline{a_n}) = (\overline{b_n})$ ist Supremum von M . Wegen $a_m \leq a_{m+i} < b_{m+i} \leq b_m$ für alle $m,i \in \mathbb{N}_0$ gilt für jedes m

$$a_m \leq (\overline{a_n}) = (\overline{b_n}) \leq b_m \ .$$

Sei jetzt $x \in \mathbb{R}$ mit $s = (\overline{b_n}) < x$, dann folgt $b_n < x$ für alle $n \geq n_0$; da b_n obere Schranke von M ist, folgt $x \notin M$. Also ist s obere Schranke von M . Sei jetzt $y \in \mathbb{R}$ mit $y < s = (\overline{a_n})$, dann gilt $y < a_n$ für alle $n \geq n_0$. Da zu a_n ein $x \in M$ mit $a_n < x$ existiert, folgt $y < a_n < x$, also ist y keine obere Schranke von M . Folglich ist s die kleinste obere Schranke von M , was zu zeigen war.

Der zweite Fall kann analog bewiesen werden. Er ergibt sich aber auch aus dem schon bewiesenen ersten Fall. Ist nämlich M eine nicht-leere nach unten beschränkte Menge, so ist die Menge U aller unteren Schranken von M nicht-leer und nach oben beschränkt. Sei t das Supremum von U , dann ist leicht zu bestätigen, daß t das Infimum von M ist. //

§ 5 Der Aufbau der reellen Zahlen mit Dedekind'schen Schnitten

Außer dem Aufbau der reellen Zahlen mit Hilfe von Cauchy-Folgen von rationalen Zahlen ist auch der Aufbau mit Hilfe von Dedekind'schen Schnitten rationaler Zahlen ein häufig verwendete Methode. Dieser Aufbau soll im folgenden durchgeführt werden.

5.1 Die Addition der reellen Zahlen

5.1.1 DEFINITION:
Eine Teilmenge $a \subset \mathbb{Q}$ der Menge der rationalen Zahlen heißt ein (D e d e k i n d ' s c h e r) S c h n i t t, wenn gelten

i) $a \neq \emptyset \wedge a \neq \mathbb{Q}$

ii) $\forall\, x \in a\ \forall\, y \in \mathbb{Q}\,[x \leq y \Longrightarrow y \in a]$

iii) a enthält kein kleinstes Element (bzgl. der Ordnung von $\mathbb{Q}$).

Die Menge der Schnitte heißt M e n g e d e r r e e l l e n Z a h l e n $\mathbb{R}$.

Die Bezeichnung der Schnitte mit kleinen lateinischen Buchstaben ist deshalb gewählt worden, weil die Schnitte im folgenden als reelle Zahlen verwendet werden. Bei schon bekanntem Aufbau der reellen Zahlen (etwa mit Hilfe von Cauchy-Folgen) entspricht einer reellen Zahl x die Menge der rationalen Zahlen, die größer als x sind. Diese Menge ist ein Schnitt. Umgekehrt kann man dann einem Schnitt diejenige reelle Zahl zuordnen, die sein Infimum ist.

Außer der oben gegebenen Definition eines Schnittes wird in der Literatur auch das Paar $(\mathbb{Q} \setminus a, a)$ bzw. nur $\mathbb{Q} \setminus a$ mit entsprechenden Axiomen als Schnitt verwendet.

5.1.2 LEMMA UND DEFINITION:
Seien a und b Schnitte. Dann ist

$$a + b := \{x + y \mid x \in a \wedge y \in b\}$$

ein Schnitt.

Beweis: i) $a \neq \emptyset \wedge b \neq \emptyset \Longrightarrow a + b \neq \emptyset$. Sei $s \notin a$, $t \notin b$, $s + t \in a + b \Longrightarrow s + t = x + y$ für $x \in a, y \in b$; wegen ii) ist $s < x$ und $t < y \Longrightarrow s + t < x + y =$ $s + t$. Widerspruch! Also ist $s + t \notin a + b$ und daher $a + b \neq \mathbb{Q}$.

ii) $x \in a \wedge y \in b \wedge x + y < z \Longrightarrow x < z - y \Longrightarrow z - y \in a \wedge$ $y \in b \Longrightarrow z = z - y + y \in a + b$.

iii) Sei $z = x + y \in a + b$ mit $x \in a, y \in b \Longrightarrow$ $\exists\, x' \in a[x' < x] \Longrightarrow x' + y < x + y \wedge x' + y \in a + b$. //

5.1.3 SATZ:
$\mathbb{R}$ zusammen mit $\mathbb{R} \times \mathbb{R} \ni (a,b) \longmapsto a + b \in \mathbb{R}$ bildet eine kommutative Gruppe.

Beweis: Assoziativität und Kommutativität folgen auf Grund der Definition der Addition direkt aus der Assoziativität bzw. Kommutativität der Addition in $\mathbb{Q}$.

Wir definieren $0^* := \mathbb{Q}^+ = \{x \mid x \in \mathbb{Q} \wedge x > 0\}$. 0^* ist offenbar ein Schnitt. Wir zeigen $a + 0^* = a$ für einen beliebigen Schnitt a. Sicherlich ist $a + 0^* \subset a$. Sei nun $x \in a$. Man wähle $y \in a$ mit $y < x$. Dann ist $x = y + (x - y) \in a + 0^*$, weil $x - y > 0$.

Für eine Teilmenge $A \subset \mathbb{Q}$ sei

$A^o := A$ falls A kein kleinstes Element besitzt

$A^o := A \setminus \{x\}$ falls x kleinstes Element von A ist.

Sei nun a ein Schnitt. Wir bilden

$$b := \{x \mid x \in \mathbb{Q} \wedge -x \notin a\}^o .$$

Zunächst zeigen wir, daß b ein Schnitt ist. Sei $y \in a$, so ist $-y \notin b$, also $b \neq \mathbb{Q}$. Sei $y \notin a$. Sei $z \in \mathbb{Q}$ mit $z < y$, dann folgt $z \notin a$. Wegen $-z, -y \in \{x \mid x \in \mathbb{Q} \wedge -x \notin a\}$ und $-y < -z$ ist $-z \in b$, also ist $b \neq \emptyset$. Sei $y \in b$ und $y < z$. Dann ist $-y \notin a$, also $-z \notin a$ und $z \in b$, d.h. es gilt ii). Hat schließlich $\{x \mid x \in \mathbb{Q} \wedge -x \notin a\}$ kein kleinstes Element, so gilt iii). Ist hingegen x_0 kleinstes Element von $\{x \mid x \in \mathbb{Q} \wedge -x \notin a\}$ und $y \in b$, so gilt $x_0 < y$, also gibt es $z \in \mathbb{Q}$ mit $x_0 < z < y$ und wegen $-z < -x_0$ ist mit $-x_0 \notin a$ auch $-z \notin a$. Folglich gibt es zu jedem $y \in b$ ein $z \in b$ mit $z < y$ und es gilt iii).

Wir zeigen nun $a + b = 0^*$. Für $x \in a$ und $y \in b$ gilt $-y \notin a$, also $-y < x$, d.h. $0 < x + y$, also $x + y \in 0^*$. Damit gilt $a + b \subset 0^*$. Sei $z \in 0^*$, d.h. $z > 0$. Sei $x \notin a$. Die Menge $\{n \mid n \in \mathbb{N}_0 \wedge x + \frac{1}{2}nz \in a\}$ ist nicht-leere Teilmenge von $\mathbb{N}_0$, denn für $y \in a$ existiert ein $n \in \mathbb{N}_0$ mit $n \cdot \frac{z}{2} > y - x$, d.h. $y < x + \frac{1}{2}nz$, also $x + \frac{1}{2}nz \in a$. Sei n_0 kleinstes Element dieser Menge. Dann gilt

$$x + \tfrac{1}{2}n_0 z \in a, \quad x + \tfrac{1}{2}(n_0 - 1)z \notin a, \quad x + \tfrac{1}{2}(n_0 - 2)z \notin a.$$

Es folgt $-(x + \frac{1}{2}(n_0 - 2)z) \in b$ und daher

$$z = x + \tfrac{1}{2}n_0 z - (x + \tfrac{1}{2}(n_0 - 2)z) \in a + b.$$

Daher gilt auch $0^* \subset a + b$. Der Satz 5.1.3 ist damit bewiesen. //

Wie üblich bezeichnen wir im folgenden $-a := b$, also $-a := \{x \mid x \in \mathbb{Q} \wedge -x \notin a\}^o$. Beachte: Dies ist nicht $\{-x \mid x \in a\}$!

Wir definieren nun eine Abbildung $\iota: \mathbb{Q} \longrightarrow \mathbb{R}$ durch $q \longmapsto \{x \mid x \in \mathbb{Q} \wedge x > q\} =: q^*$. Offenbar ist q^* für jedes $q \in \mathbb{Q}$ ein Schnitt, also in $\mathbb{R}$.

5.1.4 SATZ:
Die Abbildung

$$\iota: \mathbb{Q} \ni q \longmapsto q^* \in \mathbb{R}$$

ist ein injektiver Gruppenhomomorphismus bzgl. der Addition.

Beweis: Sei $q<p$. Dann ist $q<\frac{p+q}{2}<p$, d.h. $\frac{p+q}{2}\in q^*$ und $\frac{p+q}{2}\notin p^*$. Folglich ist $q^*\neq p^*$ und ι injektiv.

Wir zeigen $p^*+q^*=(p+q)^*$. Für $x\in p^*$, $y\in q^*$ gilt $x>p$, $y>q$, also $x+y>p+q$ und daher $x+y\in(p+q)^*$, d.h. $p^*+q^*\subset(p+q)^*$. Sei nun $x\in(p+q)^*$, $x>p+q$. Sei $y\in\mathbb{Q}$ mit $x>y>p+q$. Dann ist $y-q>p$, also $y-q\in p^*$. Weiter ist $q+x-y>q$, also $q+x-y\in q^*$. Folglich ist $x=(y-q)+(q+x-y)\in p^*+q^*$, d.h. $p^*+q^*\supset(p+q)^*$.//

5.2 Die Ordnung der reellen Zahlen

5.2.1 DEFINITION UND LEMMA:
$\mathbb{R}$ ist mit der Ordnung $a\leq b:\Longleftrightarrow b\subset a$ eine total geordnete Menge.

Beweis: Da $\subset$ auf der Potenzmenge von $\mathbb{Q}$ eine Ordnung definiert, ist $\leq$ eine Ordnung auf $\mathbb{R}$. Seien $a,b\in\mathbb{R}$ gegeben. Seien $a\neq b$. Dann gilt

$$\exists x\in\mathbb{Q}\left[(x\in a\wedge x\notin b)\vee(x\notin a\wedge x\in b)\right] .$$

Im ersten Fall gilt $x<y$ für alle $y\in b$, also $y\in a$ und damit $b\subset a$ und $a\leq b$. Im zweiten Fall gilt symmetrisch $b\leq a$. Folglich ist die Ordnung $\leq$ eine totale Ordnung. //

5.2.2 LEMMA:
Für $p,q\in\mathbb{Q}$ gilt $p<q\Longrightarrow p^*<q^*$.

Beweis: $x\in q^*\Longrightarrow x>q\Longrightarrow x>p\Longrightarrow x\in p^*$. Daraus folgt $q^*\subset p^*$, also $p^*\leq q^*$. Wegen der Injektivität von ι ist $p^*\neq q^*$, also $p^*<q^*$. //

5.2.3 SATZ (I. MONOTONIEGESETZ):
$\forall\, a,b,c\in\mathbb{R}\left[a\leq b\Longrightarrow a+c\leq b+c\right]$.

Beweis: $a \leq b \Longrightarrow b \subset a \Longrightarrow b + c \subset a + c \Longrightarrow a + c \leq b + c$ .//

5.2.4 FOLGERUNG:
$a > 0^* \Longleftrightarrow 0^* > -a$.

Beweis: $a \geq 0^* \Longleftrightarrow a + (-a) \geq 0^* + (-a) \Longleftrightarrow 0^* \geq -a$.
Ist $a \neq 0^*$, so ist auch $-a \neq 0^*$. //

5.3 Die Multiplikation der reellen Zahlen

Wir führen zunächst nur die Multiplikation von positiven reellen Zahlen ein und untersuchen ihre Eigenschaften.

5.3.1 LEMMA UND DEFINITION:
Seien $a,b \in \mathbb{R}$ und $a > 0^*$, $b > 0^*$. Dann ist

$$ab := \{xy \mid x \in a \wedge y \in b\}$$

ein Schnitt und $ab > 0^*$.

Beweis: i) $a \neq \emptyset \wedge b \neq \emptyset \Longrightarrow ab \neq \emptyset$. Da $xy > 0$ für alle $x \in a$, $y \in b$ gilt, ist $ab \neq \mathbb{Q}$.

ii) $x \in a \wedge y \in b \wedge xy < z \Longrightarrow x < zy^{-1} \Longrightarrow zy^{-1} \in a \wedge y \in b \Longrightarrow z = zy^{-1}y \in ab$.

iii) Sei $z = xy \in ab$ mit $x \in a$, $y \in b \Longrightarrow \exists\, x' \in a\,[x' < x] \Longrightarrow x'y < xy \wedge x'y \in ab$.

Wegen $a > 0^*$, $b > 0^*$ gibt es $u \notin a$, $u > 0$ und $v \notin b$, $v > 0$. Dann ist $0 < uv$ und $uv \notin ab$,also $0^* < ab$. Wäre nämlich $uv = xy \in ab$ mit $x \in a$, $y \in b$, so wäre $u < x$, $v < y$, also $uv < xy = uv$, Widerspruch! //

5.3.2 LEMMA:
$\forall\, a,b,c \in \mathbb{R}$ und $a > 0^*$, $b > 0^*$, $c > 0^*$ gelten

1) $(ab)c = a(bc)$,
2) $ab = ba$,
3) $a1^* = a$,
4) $a(b + c) = ab + ac$.

Beweis: 1), 2) und 4) gelten, weil die entsprechenden Gesetze in $\mathbb{Q}$ gelten.

3) Sei $x \in a$, $y \in 1^* \Longrightarrow y > 1 \Longrightarrow x < xy \Longrightarrow xy \in a$ $\Longrightarrow a1^* \subset a$. Sei nun $x \in a \Longrightarrow \exists y \in a [y < x] \Longrightarrow$ $1 < xy^{-1} \Longrightarrow xy^{-1} \in 1^* \Longrightarrow x = yxy^{-1} \in a1^* \Longrightarrow a \subset a1^*$. //

5.3.3 LEMMA:
$\forall a,b,c \in \mathbb{R}$ und $a > 0^*$, $b > 0^*$, $c > 0^*$ gilt

$$a \leq b \Longrightarrow ac \leq bc \ .$$

Beweis: $a \leq b \Longrightarrow b \subset a \Longrightarrow bc \subset ac \Longrightarrow ac \leq bc$. //

5.3.4 LEMMA:
$\forall a \in \mathbb{R} \left[a > 0^* \Longrightarrow \exists b \in \mathbb{R} \left[ab = 1^* \right] \right]$.

Beweis: Sei $a \in \mathbb{R}$ und $a > 0^*$. Wir bilden *)

$$b := \{x | x \in \mathbb{Q} \wedge x > 0 \wedge x^{-1} \notin a\}^o \ .$$

Zunächst zeigen wir, daß b ein Schnitt ist. Per Definition ist $b \neq \mathbb{Q}$. Wegen $a > 0^*$ existiert ein $y \notin a$ mit $y > 0$. Dann gibt es ein $z > 0$ mit $z < y$, also $z \notin a$. Wegen $y^{-1}, z^{-1} \in \{x | x \in \mathbb{Q} \wedge x > 0 \wedge x^{-1} \notin a\}$ und $y^{-1} < z^{-1}$ ist $z^{-1} \in b$, also ist $b \neq \emptyset$. Sei $y \in b$ und $y < z$. Dann ist $y^{-1} \notin a$, also auch $z^{-1} \notin a$ wegen $z^{-1} < y^{-1}$, und $z \in b$, d.h. es gilt ii). Hat schließlich $\{x | x \in \mathbb{Q}\ x > 0\ x^{-1} \notin a\}$ kein kleinstes Element, so gilt iii). Ist hingegen x_o kleinstes Element dieser Menge und $y \in b$, so gilt $x_o < y$, also gibt es ein $z \in \mathbb{Q}$ mit $x_o < z < y$. Wegen $z^{-1} < x_o^{-1}$ ist mit $x_o^{-1} \notin a$ auch $z^{-1} \notin a$. Folglich gibt es zu jedem $y \in b$ ein $z \in b$ mit $z < y$, und es gilt iii).

Wir zeigen nun $ab = 1^*$. Für $x \in a$ und $y \in b$ gilt $y^{-1} \notin a$, also $y^{-1} < x$, d.h. $1 < xy$ und $xy \in 1^*$. Damit gilt $ab \subset 1^*$.

Die Umkehrung $1^* \subset ab$ zeigen wir in drei Schritten. Sei $x \in 1^*$. Dann gibt es ein $y \in \mathbb{Q}$ mit $1 < y < x$.

---

*) Zur Definition von $\{...\}^o$ vgl. Beweis von 5.1.3

1. Behauptung: Für alle $n \in \mathbb{N}_0$ gilt $1 + n(y-1) \leq y^n$.
Für $n = 0$ ist dies klar. Ist nun $1 + n(y-1) \leq y^n$, so ist $y^{n+1} = y^n(1 + (y-1)) \geq (1 + n(y-1))(1 + (y-1)) \geq 1 + (n+1)(y-1)$.

2. Behauptung: Es gibt ein $z \in a$ mit $y^{-1}z \notin a$.
Wäre nämlich $y^{-1}z \in a$ für alle $z \in a$, so wäre insbesondere $y^{-n}z_0 \in a$ für ein $z_0 \in a$ und alle $n \in \mathbb{N}_0$ (durch Induktion). Ist aber $u \in \mathbb{Q}$, $u > 0$, so gibt es nach 3.3.2 ein $n \in \mathbb{N}$ mit $n(y-1) > u^{-1}z_0 - 1$
$\Longrightarrow 1 + n(y-1) > u^{-1}z_0 \Longrightarrow y^n > u^{-1}z_0 \Longrightarrow u > y^{-n}z_0 \in a$
$\Longrightarrow u \in a \Longrightarrow a = 0^*$ im Widerspruch zur Voraussetzung.

3. Behauptung: $x \in ab$.
Sei $z \in a$ mit $y^{-1}z \notin a$. $z > 0 \wedge y < x \Longrightarrow x^{-1} < y^{-1} \wedge x^{-1}z < y^{-1}z \Longrightarrow x^{-1}z \notin a \wedge (y^{-1}z)^{-1} < (x^{-1}z)^{-1} \Longrightarrow (x^{-1}z)^{-1} \in b \Longrightarrow x = z(x^{-1}z)^{-1} \in ab$. //

Wie üblich bezeichnen wir für $a > 0^*$ das im Beweis von 5.3.4 angegebene b mit a^{-1}, also

$$a^{-1} := \{x \mid x \in \mathbb{Q} \wedge x > 0 \wedge x^{-1} \notin a\}^o .$$

Wir setzen nun die Multiplikation von den positiven reellen Zahlen auf ganz $\mathbb{R}$ fort.

5.3.5 DEFINITION:
1) Für $a \in \mathbb{R}$ sei

(i) $$|a| := \begin{cases} a & \text{falls } a \geq 0^* \\ -a & \text{falls } a < 0^* \end{cases}$$

(ii) $$\operatorname{sgn}(a) := \begin{cases} 1 \in \mathbb{Z} & \text{falls } a > 0^* \\ 0 \in \mathbb{Z} & \text{falls } a = 0^* \\ -1 \in \mathbb{Z} & \text{falls } a < 0^* \end{cases}$$

(iii) $1 \circ a := a$, $0 \circ a := 0^*$ und $(-1) \circ a := -a$.

2) Für $a, b \in \mathbb{R}$ sei

$$a \cdot b := (\operatorname{sgn}(a)\operatorname{sgn}(b)) \circ (|a|\,|b|) .$$

3) Für $a \neq 0^*$ sei

$$a^{-1} := \operatorname{sgn}(a) \circ |a|^{-1} .$$

Wir machen im folgenden eine Reihe von Bemerkungen, deren Beweise meist sofort klar sind.

BEMERKUNGEN:

(1) Die vorstehende Definition der Multiplikation stimmt für $a > 0^*$, $b > 0^*$ mit der in 5.3.1 definierten Multiplikation überein, denn für $a > 0^*$ gilt $sgn(a) = 1$ und $|a| = a$.

(2) $a0^* = 0^*a = 0^*$ für alle $a \in \mathbb{R}$.

(3) $a = sgn(a) \circ |a|$, $|a| = |-a|$, $sgn(-a) = -sgn(a)$ für alle $a \in \mathbb{R}$.

(4) $|a||b| > 0^*$ für $a \neq 0^*$, $b \neq 0^*$ (nach 5.2.4 und 5.3.1).

(5) $a \cdot b = 0^* \Longrightarrow a = 0^* \vee b = 0^*$ für $a,b \in \mathbb{R}$.

(6) $|a \cdot b| = (sgn(a)sgn(b)) \circ (|a||b|) = |a| \cdot |b|$.

(7) $sgn(a \cdot b) = sgn((sgn(a)sgn(b)) \circ (|a||b|)) =$
$= sgn(a)sgn(b)$ für alle $a,b \in \mathbb{R}$.

(8) $sgn(-(a \cdot b)) = -sgn(a \cdot b) = -sgn(a)sgn(b) =$
$= sgn(-a)sgn(b) = sgn(a)sgn(-b)$ für alle $a,b \in \mathbb{R}$.

(9) $-(a \cdot b) = sgn(-(a \cdot b)) \circ |a \cdot b| = sgn(-(a \cdot b)) \circ (|a||b|)$
$= (sgn(-a)sgn(b)) \circ (|-a||b|) = (-a) \cdot (b)$
$= (sgn(a)sgn(-b)) \circ (|a||-b|) = (a) \cdot (-b)$ für alle $a,b \in \mathbb{R}$.

Wir benutzen diese Eigenschaften ohne besondere Erwähnung. Wegen (1) können wir die Multiplikation ohne Multiplikationspunkt schreiben: $ab = a \cdot b$.

5.3.6 SATZ:
$(\mathbb{R},+,\cdot,=)$ ist ein angeordneter Körper.

Beweis: 1) $(ab)c = ((sgn(a)sgn(b))sgn(c)) \circ ((|a||b|)|c|)$
$= a(bc)$.

2) $ab = (sgn(a)sgn(b)) \circ (|a||b|) = ba$.

3) $a(b + c) = ab + ac$: Sei zunächst $a > 0^*$. Für $b \geq 0^*$, $c \geq 0^*$, $b \geq c$ gilt

$a(b + c) = ab + ac$
$a(b - c) = a(b - c) + ac - ac = a(b - c + c) - ac = ab + a(-c)$
$a(-b + c) = -(a(b - c)) = -(ab - ac) = -(ab) + ac$

$= a(-b) + ac$

$a(-b - c) = -(a(b + c)) = -(ab + ac) = a(-b) + a(-c)$.

Ist $a = 0^*$, so gilt $a(b + c) = 0^* = ab + ac$.

Ist $a < 0^*$, so gilt $a(b + c) = -((-a)(b + c)) =$
$-((-a)b + (-a)c) = ab + ac$.

4) $a1^* = \mathrm{sgn}(a) \circ (|a| 1^*) = \mathrm{sgn}(a) \circ |a| = a$.

5) Für $a \neq 0^*$ gilt $aa^{-1} = (\mathrm{sgn}(a)\mathrm{sgn}(a)) \circ (|a|\,|a|^{-1})$
$= 1^* = a^{-1}a$.

6) (II. Monotoniegesetz) Sei $a \geq 0^*$ und $b \leq c$. Dann
ist $c - b \geq 0^*$, also $0^* \leq a(c - b) = ac - ab \Longrightarrow ab \leq ac$. //

5.3.7 SATZ:
Für $p,q \in \mathbb{Q}$ gilt $(pq)^* = p^*q^*$.

Beweis: Seien zunächst $p > 0$, $q > 0$. Dann gilt
$x \in p^*$, $y \in q^* \Longrightarrow xy > pq \Longrightarrow xy \in (pq)^*$, also
$p^*q^* \subset (pq)^*$. Sei umgekehrt $z \in (pq)^*$. Dann gilt
$z > pq \Longrightarrow \exists\, z' [pq < z' < z] \Longrightarrow z'p^{-1} > q \Longrightarrow z'p^{-1} \in q^*$;
weiter gilt $zz'^{-1}p > p$, also $z = zz'^{-1}pz'p^{-1} \in p^*q^*$
und damit $(pq)^* \subset p^*q^*$.

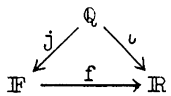
Sind $p = 0$ oder $q = 0$, so gilt $(pq)^* = 0^* = p^*q^*$.
Sind $p < 0$ oder $q < 0$, so kann man die Vorzeichen
gesondert betrachten und erhält ebenfalls $(pq)^* = p^*q^*$. //

5.4 Vergleich der beiden Konstruktionen von reellen Zahlen

In diesem Abschnitt wollen wir zeigen, daß beide angegebenen Konstruktionen von reellen Zahlen, die mit Cauchy-Folgen und die mit Dedekind'schen Schnitten, zu demselben Begriff des Körpers der reellen Zahlen führen. Da die Definition einer reellen Zahl durch Cauchy-Folgen bzw. Dedekind'sche Schnitte zu verschiedenen mathematischen Objekten führt, können wir nur erwarten, daß die so konstruierten Körper isomorph sind. Zur Bezeichnung des Körpers der reellen Zahlen, der mit Cauchy-Folgen konstruiert ist, wollen wir in diesem Abschnitt das Zeichen $\mathbb{F}$ verwenden. Weiter nehmen wir an, daß $\mathbb{Q}$ mit der entsprechenden Teil-

menge von $\mathbb{F}$ identifiziert ist. Wir bezeichnen die Inklusionsabbildung von $\mathbb{Q}$ in $\mathbb{F}$ durch $j:\mathbb{Q} \longrightarrow \mathbb{F}$.

5.4.1 SATZ:
Es gibt genau einen ordnungstreuen Körperisomorphismus $f: \mathbb{F} \longrightarrow \mathbb{R}$, so daß



kommutativ ist. (ι im Sinne von 5.1.4)

Beweis: Sei $r \in \mathbb{F}$. Wir definieren $f(r) := \{x \mid x \in \mathbb{Q} \wedge x > r\}$. (Beachte $x = j(x)$!) $f(r)$ ist trivialerweise ein Schnitt. Weiter definieren wir $g: \mathbb{R} \longrightarrow \mathbb{F}$ durch $g(a) := \inf(a)$, das Infimum der Teilmenge $a \subset \mathbb{F}$ (genauer $g(a) = \inf\{j(x) \mid x \in a\}$). $\inf(a)$ existiert, weil a nach unten beschränkt und nicht leer ist. Wir zeigen $g = f^{-1}$. Sei zunächst $a \in \mathbb{R}$ und $x \in a$. Dann ist $x > \inf(a)$, da a kein kleinstes Element besitzt. Also ist $x \in fg(a)$, und wir haben $a \subset fg(a)$. Sei $x \in fg(a)$, d.h. $x > \inf(a)$. Dann existiert $y \in a$ mit $x > y > \inf(a) \Longrightarrow x \in a$. Daher gilt $fg(a) \subset a$ und folglich $a = fg(a)$. Wir zeigen nun $r = gf(r)$. Sei $r \in \mathbb{F}$, dann ist $r \leq \inf\{x \mid x \in \mathbb{Q} \wedge x > r\} = gf(r)$. Ist aber $r < gf(r)$, so gibt es ein $x \in \mathbb{Q}$ mit $r < x < gf(r)$ im Widerspruch zu $gf(r) = \inf\{x \mid x \in \mathbb{Q} \wedge x > r\}$. Damit gilt $r = gf(r)$ und $g = f^{-1}$.

Wir zeigen jetzt $fj = \iota$. Sei $x \in \mathbb{Q}$, $x = j(x)$. Dann ist $fj(x) = f(x) = \{y \mid y \in \mathbb{Q} \wedge y > x\} = x^* = \iota(x)$.

Um zu zeigen, daß f ein ordnungstreuer Körperhomomorphismus ist, seien $r,s \in \mathbb{F}$. Dann gilt wie leicht zu sehen

$$\begin{aligned} f(r+s) &= \{x \mid x \in \mathbb{Q} \wedge x > r+s\} \\ &= \{u+v \mid u,v \in \mathbb{Q} \wedge u > r \wedge v > s\} \\ &= f(r) + f(s) \end{aligned}$$

$$\begin{aligned} f(rs) &= f((\mathrm{sgn}(r)\mathrm{sgn}(s)) \circ (|r||s|)) \\ &= (\mathrm{sgn}(r)\mathrm{sgn}(s)) \circ f(|r||s|) \\ &= (\mathrm{sgn}(r)\mathrm{sgn}(s)) \circ \{x \mid x \in \mathbb{Q} \wedge x > |r||s|\} \end{aligned}$$

$$= (\mathrm{sgn}(r)\mathrm{sgn}(s))\circ\{uv \mid u,v \in \mathbb{Q} \wedge u > |r| \wedge v > |s|\}$$
$$= (\mathrm{sgn}(r)\mathrm{sgn}(s))\circ f(|r|)f(|s|)$$
$$= f(r)f(s) \ ,$$

wobei wir verwendet haben $f(-r) = -f(r)$ und $f(0) = 0^*$. Sei $r \leq s$. Dann ist $\{x \mid x \in \mathbb{Q} \wedge x > r\} \supseteq \{x \mid x \in \mathbb{Q} \wedge x > s\}$, also $f(r) \leq f(s)$.

Ist auch f' ein ordnungstreuer Körperisomorphismus mit $f'j = \iota$, so ist $f^{-1}f' = h$ ein ordnungstreuer Körperautomorphismus von $\mathbb{F}$ mit $hj = f^{-1}f'j = f^{-1}\iota = j$, also $h|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Sei $r \in \mathbb{F}$ mit $h(r) = s \neq r$. Wir können annehmen $s < r$. Im anderen Falle wähle h^{-1} statt h . Wegen $s < r$ gibt es ein $x \in \mathbb{Q}$ mit $s < x < r$, also $x = h(x) < h(r) = s$ im Widerspruch zu $s < x$. Daher ist $h = \mathrm{id}_{\mathbb{F}}$ und $f' = f$. //

5.4.2 FOLGERUNG:
Die identische Abbildung ist der einzige ordnungstreue Körperautomorphismus von $\mathbb{R}$.

Beweis: Im Beweis von 5.4.1 haben wir gezeigt, daß ein ordnungstreuer Körperautomorphismus $h: \mathbb{R} \longrightarrow \mathbb{R}$ die Identität ist, falls seine Einschränkung auf $\mathbb{Q}$ die Identität auf $\mathbb{Q}$ induziert. Es genügt also zu zeigen, daß jeder Körperhomomorphismus $h: \mathbb{Q} \longrightarrow \mathbb{R}$ die Einbettung von $\mathbb{Q}$ in $\mathbb{R}$ ist. Da $h(1) = 1$, ist für alle $n \in \mathbb{Z} \subset \mathbb{Q}$ auch $h(n) = n$, denn h ist ein Körperhomomorphismus. Für $\frac{m}{n} \in \mathbb{Q}$ mit $m,n \in \mathbb{Z}$ gilt $h(\frac{m}{n}) = \frac{h(m)}{h(n)} = \frac{m}{n}$, also ist h die Einbettung . //

§ 6 Die komplexen Zahlen

In diesem kurzen Abschnitt soll die Definition des Körpers der komplexen Zahlen gegeben werden. Wir beweisen, daß $\mathbb{R}\times\mathbb{R}$ mit der Addition

$$(x,y) + (x',y') := (x + x', y + y')$$

und der Multiplikation

$$(x,y)(x',y') := (xx' - yy', xy' + x'y)$$

einen kommutativen Körper bildet, den Körper $\mathbb{C}$ der komplexen Zahlen.

Es ist klar, daß $\mathbb{R}\times\mathbb{R}$ mit der Addition eine kommutative Gruppe bildet. Die Ringeigenschaften von $\mathbb{C}$ lassen sich durch Nachrechnen leicht verifizieren. Das neutrale Element bei der Multiplikation ist dabei $(1,0)$. Inverses Element zu $(x,y) \neq (0,0)$ ist

$$(x,y)^{-1} := \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2}\right) .$$

Auch das kann sofort nachgerechnet werden.

Die Abbildung $\mathbb{R} \ni x \longmapsto (x,0) \in \mathbb{C}$ ist ein injektiver Ringhomomorphismus. Daher identifiziert man $\mathbb{R}$ mit dem Unterkörper $\{(x,0) \mid x \in \mathbb{R}\}$ in $\mathbb{C}$.

Üblicherweise schreibt man $i := (0,1)$ und allgemein $x + yi = (x,y)$. Insbesondere ist dann

$$i^2 = -1 .$$

Es liegt die Frage nahe, ob man die Ordnung von $\mathbb{R}$ auf $\mathbb{C}$ fortsetzen kann, so daß dann $\mathbb{C}$ ein angeordneter Körper wäre. Dies ist nicht der Fall! In $\mathbb{R}$ gilt $-1 < 0$. In einem angeordneten Körper K gilt, wie in 3.2.4 festgestellt, $0 \leq x^2$ für jedes $x \in K$. Für $x = i \in \mathbb{C}$ folgte $-1 < 0 \leq i^2 = -1$, Widerspruch!

Eine grundlegende Eigenschaft des Körpers der komplexen Zahlen, die als Fundamentalsatz der Algebra formuliert wird, wird üblicherweise in der Funktionentheorie bewiesen. Sie besagt, daß man jedes Polynom $P(x) \in \mathbb{C}[x]$ vom Grad $n \geq 1$ in der Form

$$P(x) = a(x - b_1)(x - b_2)\ldots(x - b_n)$$

mit $a, b_1, \ldots, b_n \in \mathbb{C}$ schreiben kann. Es gibt also in $\mathbb{C}[x]$ keine irreduziblen Polynome von einem Grad > 1. Man sagt dafür auch, daß $\mathbb{C}$ algebraisch abgeschlossen ist. Daraus folgt auch, daß es keinen Oberkörper von $\mathbb{C}$ gibt, der als $\mathbb{C}$-Vektorraum endliche Dimension besitzt. Allerdings gibt es einen (und nur einen) Oberschiefkörper endlicher Dimension von $\mathbb{C}$.

§ 7 Die Quaternionen

Der Körper $\mathbb{C}$ der komplexen Zahlen besitzt einen Automorphismus $\mathbb{C} \ni z \longmapsto z^* \in \mathbb{C}$, genannt Konjugation, der wie folgt definiert wird. Für $z = (x,y)$ mit $x,y \in \mathbb{R}$ sei $z^* := (x,-y)$. Es gilt nämlich für $z = (x,y)$, $t = (u,v)$

$$(z+t)^* = ((x,y)+(u,v))^* = (x+u,y+v)^*$$
$$= (x+u,-y-v)^* = (x,-y)+(u,-v) = z^* + t^* ,$$

$$(zt)^* = ((x,y)(u,v))^* = (xu-yv,xv+yu)^*$$
$$= (xu-yv,-xv-yu) = (x,-y)(u,-v) = z^*t^* .$$

Offenbar gilt $z^{**} = z$, so daß die Konjugation ein Automorphismus ist. Weiter ist $zz^* = (x,y)(x,-y) = (x^2+y^2,0) \in \mathbb{R}$, also gilt $z \neq 0 \Longrightarrow zz^* > 0$ in $\mathbb{R}$.

Sei $\mathbb{H} := \mathbb{C} \times \mathbb{C}$. Wir definieren

(*) $\quad (z,t)+(z',t') := (z+z',t+t')$

und

(**) $\quad (z,t)(z',t') := (zz'-t^*t',z^*t'+tz')$.

$\mathbb{H}$ mit der Addition (*) bildet eine kommutative Gruppe, da $\mathbb{H}$ sogar ein $\mathbb{C}$-Vektorraum ist. Für die Multiplikation (**) gelten Assoziativ- und Distributiv-Gesetze, wie man leicht nachrechnet. Weiter gelten

1) $(1,0)(z,t) = (z,t) = (z,t)(1,0)$.

2) Sei $(z,t) \neq (0,0)$. Dann gilt $zz^* + tt^* > 0$ in $\mathbb{R}$ und $(z,t)\left(\frac{z^*}{zz^*+tt^*},\frac{-t}{zz^*+tt^*}\right) = \left(\frac{zz^*+tt^*}{zz^*+tt^*},\frac{-z^*t+tz^*}{zz^*+tt^*}\right)$
$= (1,0)$.

3) $(i,0)(0,1) = (0,-i) \neq (0,i) = (0,1)(i,0)$, d.h. die Multiplikation in $\mathbb{H}$ ist nicht kommutativ.

Wir haben damit folgende Aussage bewiesen:

7.1 SATZ und DEFINITION:
$\mathbb{H}$ zusammen mit der Addition (*) und der Multiplikation (**) ist ein Schiefkörper, der Schiefkörper der Quaternionen.

Man sieht leicht, daß $\mathbb{C} \ni z \longmapsto (z,0) \in \mathbb{H}$ ein Körperhomomorphismus ist, so daß $\mathbb{C}$ als Unterkörper von $\mathbb{H}$ aufgefaßt werden kann.

Folgende Bezeichnungen sind üblich:

$1 := (1,0)$, $i := (i,0)$, $j := (0,1)$, $k := (0,-i)$.

Dann sind $1,i,j,k$ eine $\mathbb{R}$-Basis für den $\mathbb{R}$-Vektorraum $\mathbb{H}$. Weiter gelten

$$i^2 = j^2 = k^2 = -1 ,$$

$$ij = k = -ji ,$$

$$jk = i = -kj ,$$

$$ki = j = -ik .$$

Stichwortregister